UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
SOUTHERN DIVISION

IN RE: MARRIOTT INTERNATIONAL, INC., CUSTOMER DATA SECURITY BREACH LITIGATION	MDL No. 19-md-2879 Judge Paul W. Grimm
This Document Relates To: DENNIS MCGRATH, Individually and on behalf of all others similarly situated, Plaintiff, vs. MARRIOTT INTERNATIONAL, INC., ARNE M. SORENSON, KATHLEEN KELLY OBERG, BAO GIANG VAL BAUDUIN, BRUCE HOFFMEISTER, and STEPHANIE C. LINNARTZ, Defendants.	This document relates to Case No. 8:19-cv-00368-PWG **JURY TRIAL DEMANDED**

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT
FOR VIOLATIONS OF FEDERAL SECURITIES LAWS

TABLE OF CONTENTS

By and through its undersigned counsel, Construction Laborers Pension Trust for Southern California ("Southern California Laborers" or "Lead Plaintiff") brings this complaint individually, and on behalf of a class of similarly situated persons and entities, against Defendant Marriott International, Inc. ("Marriott" or the "Company") and Defendants Arne M. Sorenson, Kathleen Kelly Oberg, Bao Giang Val Bauduin, Bruce Hoffmeister, and Stephanie C. Linnartz (together, the "Individual Defendants," and collectively with Marriott, the "Defendants").

Lead Plaintiff alleges the following upon personal knowledge as to those allegations concerning Lead Plaintiff and, as to all other matters, upon the investigation of counsel, which included, without limitation: (a) review and analysis of public filings made by Marriott with the U.S. Securities and Exchange Commission ("SEC"); (b) review and analysis of press releases and other publications, including those disseminated by certain of the Defendants and other related non-parties; (c) review of news articles; (d) review of materials from other litigation arising as a result of The Breach; (e) interviews with former employees of Marriott and Starwood Hotels and Resorts Worldwide, Inc. ("Starwood"), its affiliates and predecessors, and other third parties; and (f) consultation with individuals with expertise in cybersecurity, information technology systems, and damages. Lead Plaintiff believes that substantial additional evidentiary support exists for the allegations herein that will be revealed after Lead Plaintiff has a reasonable opportunity to conduct discovery.

I. NATURE OF THE CLAIM

1. Marriott is now the largest hotel company in the world. But back in 2015, Marriott's growth was waning and its stock price was slumping, along with that of its competitors. This general downward trend in the hotel industry was fueled by the emergence and dominance of two sources of pressure. First, sites such as Airbnb or VRBO allowed customers to book non-traditional, hotel-like properties, oftentimes at a lower rate than traditional hotels

like Marriott. Second, online travel agencies, like Expedia or Travelocity, offer hotel rooms for sale – including Marriott's – but they do it for a fee. Marriott both competed with these sites with direct booking through its own sites, and negotiated with these sites so at least some of the Company's rooms would be available through these websites. Analysts saw these competitors as posing a danger to hotel companies, with an analyst from Barclays identifying Airbnb as a "longer-term threat" to the hotel industry's revenues.

2. So, in mid-2015, Marriott sought to consolidate power and grow its business by merging with another hotel company – Starwood (the "Merger"). Starwood was known for its younger, high-end clientele and business travelers, and was famous for its loyalty program, which provided customers with rewards – such as free nights – for staying at Starwood properties.

3. But this transformational acquisition was the biggest merger that the hotel industry had ever seen, and the largest merger that Marriott had ever attempted. Up until the Merger, Marriott had acquired smaller hotel chains in "tuck-in" acquisitions of approximately $100 to $200 million dollars with hotel chains that had, at a maximum, 160 hotels. The acquisition of Starwood, however, was massive, ***valued at $13 billion dollars, with Starwood properties numbering in the thousands.***

4. One of the most important parts of the Merger involved acquiring Starwood's guest reservation database and loyalty program data. This information was valuable to Marriott because it would allow Marriott to market to these customers, and broaden Marriott's dominance and reach among a wider range of customers. Marriott hoped to harness the power of these customers and leverage the customer data it purchased from Starwood to not only gain market share, but to drive revenues up as well.

5. Analysts understood the importance of acquiring customer data for Marriott's investors, and also the positive effect this could have for Marriott *vis-à-vis* its non-traditional competition. For example, an analyst at Macquarie stated: "Investors should also acknowledge that access to a more diverse client base will generate even more valuable customer data and should improve marketing efforts, especially towards younger and more tech savvy groups. We also see combined marketing and sales strategies as being a strong advantage over [online travel agencies] and other hotels."

6. Overall, analysts were excited about the Merger and touted the growth that it would bring for Marriott. For example, an analyst from Credit Suisse stated "[w]e believe MAR will be able to unlock significant value from the acquisition," and "[t]here is no disputing that a combined MAR/HOT entity will create a strong #1 player in the industry."

7. Marriott touted the importance of data for the Company by calling it a "tremendous asset," and also understood the importance of keeping that data secure. Marriott assured the market that "the integrity and protection" of customer data was "critical" to the Company, and indeed, Marriott was subject to numerous regulations that required it to protect its customer data. So, when Marriott sought to merge with Starwood, it knew that keeping the customer data it was about to purchase was of the utmost importance.

8. At the outset, Defendants assured the market that they were performing "extensive" due diligence and working on the successful integration of the two companies. Defendants also repeatedly assured investors that Marriott's prior merger experience set them up to execute this acquisition successfully as well. Marriott even told the market that based on "the results of Marriott's due diligence review of Starwood, the prospects for the combined company [were] favorable." Defendant also continuously touted "joint integration planning" with

Starwood, multiple meetings between the two companies, Board involvement in the due diligence process, and the "exhaustive planning" surrounding the Merger and the integration process. Based on this due diligence, Marriott told the market that the integration was "on track," and did not foresee any issues with a successful integration.

9. However, there were significant issues. Former employees and contractors for both Starwood and Marriott collectively confirm that Starwood's network was extremely vulnerable and Marriott knew it.

10. A Senior Global Cyber-Security Consultant at Starwood explained that Starwood used a very antiquated version of the Oracle application portal for its information technology ("IT") system, which contained over 150 applications, including the Starwood's Reservation and SPG Loyalty Points systems. He explained that Starwood refused to pay Oracle for maintenance support for years, so "nothing was updated or patches implemented to prevent hacking." This former Starwood consultant also said this left Starwood's Oracle application portal seven years past its end of life and very vulnerable to attack by hackers.

11. A former employee who was part of senior leadership at Marriott and a Senior Director at Marriott's corporate headquarters in Bethesda, Maryland (and who ultimately reported to Defendant Hoffmeister) said that the general consensus amongst Marriott leadership was that there was a high "likelihood of a threat." This former employee from Marriott corroborates the Starwood consultant's statement, saying Starwood's Oracle stack was beyond being patched and it would have cost hundreds of millions of dollars to fix. He explained that the stack was at capacity and could no longer be patched or expanded upon. Unsurprisingly, this former employee in senior leadership at Marriott said, "Marriott was aware of the security flaws

both before, during and after the acquisition" and that the due diligence process was "one of the ways we found out" about the weaknesses in Starwood's system.

12. According to a former Software Developer and Technical Lead for Marriott, Marriott knew it was vulnerable as a result of the Starwood acquisition and that Starwood's IT department had "poor security hygiene."

13. Even after the acquisition was completed in September of 2016, Marriott continued to tout the integration, but former employees of Marriott tell another story - one of Marriott being "house poor" following the Starwood acquisition because Marriott had spent so much money on the acquisition that they did not have the money to invest in resources such as products to measure and assess IT security, and one where senior management would often reject proposals for IT spending outright, without entertaining the proposal. But Marriott doubled down, despite Starwood's obviously vulnerable system, claiming it used "sophisticated technology and systems" in the Company's reservation management system (which now included Starwood's system).

14. In September of 2018, Marriott discovered that the legacy Starwood reservation database had been hacked as of 2014 (the "Breach") – meaning the hack existed at the time Marriott supposedly conducted "extensive" and "exhaustive" due diligence. This was not a surprise internally at Marriott, of course, given the terrible state of Starwood's cybersecurity system, which one former consultant at Starwood says was "wide open," "a joke," and "Swiss cheese." But despite finding out about the Breach, Marriott kept quiet, and continued to operate Starwood's breached guest reservation system, putting its millions of customers at risk.

15. Marriott finally came clean on November 30, 2018, when the Company revealed that attackers had stolen: (1) names; (2) passport numbers; (3) dates of birth; (4) credit card

information; (5) home addresses; and (6) other valuable, sensitive personal information ***from over 500 million customers.*** Marriott finally explained to the market that they had failed to discover the Breach for the past two years and had failed to discover it during the "extensive" due diligence process as well. The market was shocked. As a result of these revelations, Marriott's stock dropped by $6.81 from a close of $121.84 per share on November 29, 2018 to $115.03 per share on November 30, 2018, a decline of 5.59%, which harmed investors.

16. Investigations into this massive breach commenced, including those by Attorneys General, the Federal Trade Commission ("FTC") and others. Commentary around the Breach included statements such as "a company can claim to take security seriously, but they don't if you can be hacked over a four-year period without noticing." Forbes questioned "why [the Company] only now detected a problem that evidently began four years ago." A Senate subcommittee was convened where Senator Carper said that Marriott "acquired a company with 'serious cybersecurity challenges and had actually been attacked before' but chose to initially leave Starwood's system in place after acquiring it." The European Union's Information Commissioner's Office ("ICO"), an agency in the UK which regulates European data laws, damningly found after its investigation that "***Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems."*** Moreover, Marriott is subject to certain regulations through the Payment Card Industry ("PCI") because they transact with credit card numbers. An investigation into whether PCI standards were violated also confirmed Marriott's deficient data security practices. Marriott's extensive failures in both the acquisition of Starwood and its continued operation of the obviously deficient reservation database (despite its critical importance to the Company) ultimately harmed investors and the Class.

II. JURISDICTION AND VENUE

17. This complaint alleges claims which arise under (1) Section 10(b) of the Securities Exchange Act (the "Exchange Act"), 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC, 17 C.F.R. § 240.10b-5; and (2) Section 20(a) of the Exchange Act, 15 U.S.C. § 78t(a).

18. This court has subject matter jurisdiction over this action pursuant to Section 27 of the Exchange Act, 15 U.S.C. § 78aa, and 28 U.S.C. § 1331. During the Class Period, as defined below, Marriott was incorporated in the state of Delaware, listed its stock on the NASDAQ and Chicago Stock Exchange, and maintained its global headquarters in Bethesda, Maryland. During the Class Period: (1) Defendant Sorenson was, and continues to be, the CEO of Marriott; (2) Defendant Oberg was, and continues to be, the Chief Financial Officer ("CFO") of Marriott as well as Manager of Starwood; (3) Defendant Val Bauduin was, and continues to be, the Chief Accounting Officer ("CAO") of Marriott as well as Vice President ("VP") and Manager of Starwood; (4) Defendant Bruce Hoffmeister was, and continues to be, Marriott's Chief Information Officer ("CIO"); and (5) Defendant Linnartz was, and continues to be, Marriott's Global Chief Commercial Officer ("CCO") and Executive VP.

19. Venue is proper in this judicial district pursuant to Section 27 of the Exchange Act, 15 U.S.C. § 78aa, and 28 U.S.C. § 1391(b). Marriott maintains its global headquarters in Bethesda, Maryland, which includes the Company's executive offices. During the Class Period, each of the Individual Defendants was a member of Marriott's senior management. In connection with the acts alleged in this complaint, Defendants, directly, or indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the mails, interstate telephone communications, interstate email communications, and the facilities of the NASDAQ and the Chicago Stock Exchange.

III. PARTIES

A. Lead Plaintiff

20. Southern California Laborers is a multi-employer pension plan with more than 31,000 participants, and approximately $1.8 billion in assets, located in El Monte, California. As set forth in its Certification previously filed in this action, (ECF No. 210), which is incorporated by reference herein, Lead Plaintiff acquired thousands of shares of Marriott's securities and incurred substantial losses as a result of Defendants' actions.

B. Defendants

21. During the Class Period, Defendant Marriott was a publicly traded company, listed on the NASDAQ and the Chicago Stock Exchange under the ticker MAR. It is incorporated in Delaware, with its headquarters in Bethesda, Maryland, and has offices in Gaithersburg, Maryland. Marriott is a worldwide operator, franchisor, and licensor of hotel, residential, and timeshare properties. As of the time it released its 2018 Annual Report, Marriott had over 2,000 properties with more than 550,000 rooms operating under thirty different brands. In Fiscal Year ("FY") 2018, the Company had annual revenues of more than $20.7 billion, as well as operating income of more than $2.3 billion. As a result of the Merger, Starwood became a wholly owned subsidiary of Marriott. Accordingly, on September 23, 2016, Marriott subsumed Starwood's assets, liabilities, and operations.

22. Defendant Arne M. Sorenson ("Sorenson") is Marriott's CEO and President. Defendant Sorensen has been CEO since March 2012 and President since May 2009. Defendant Sorenson has been a member of Marriott's Board of Directors since 2011 and currently serves on the Board's Committee for Excellence and the Executive Committee. Prior to becoming CEO, Defendant Sorenson was Marriott's COO from May 2009 to March 2012 and was CFO from 1998 to May 2009. Defendant Sorenson started with Marriott in 1996 and has served in a

number of additional roles with the Company, including Senior Vice President of Business Development, working on M&A, and Principal Accounting Officer. Defendant Sorenson's relationship with Marriott goes back to at least 1992 when he worked with the Company during his time as an M&A attorney with Latham and Watkins. During the Class Period, Defendant Sorenson signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood.

23. Defendant Kathleen Kelly Oberg ("Oberg") is Marriott's CFO and an Executive VP. Defendant Oberg has been in these roles since January 2016. Prior to becoming CFO of Marriott, Defendant Oberg was CFO of the Ritz-Carlton Hotel Company L.L.C., a Marriott subsidiary. Defendant Oberg started with Marriott in 1999 and has served in a number of roles with the Company, including Senior VP, Corporate and Development Finance and Senior VP of International Project Finance and Asset Management. Defendant Oberg has also been Manager of Starwood since September 2016, when Marriott acquired Starwood. During the Class Period, Defendant Oberg signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood.

24. Defendant Bao Giang Val Bauduin ("Val Bauduin") is Marriott's CAO and Controller. Defendant Val Bauduin has been in these roles since June 2014. Prior to becoming CAO of Marriott, Defendant Val Bauduin was a partner at Deloitte & Touche LLP. Defendant Val Bauduin has also been Vice President and Manager of Starwood since September 2016. As a part of his role as CAO, Defendant Val Bauduin is responsible for oversight of Financial Reporting and Analysis, Accounting Policy, Governance, Risk Management, Accenture Hospitality Services, and Corporate Finance Business Partners. During the Class Period, Defendant Val Bauduin signed SEC filings on behalf of Marriott.

25. Defendant Bruce Hoffmeister ("Hoffmeister") is Marriott's CIO. Defendant Hoffmeister has been in his current role with the Company since April 2011. Prior to assuming his current role, Defendant Hoffmeister was a Senior VP: IR Shared and Application Services and a Senior VP, Global Revenue Management, in addition to holding various other finance and accounting roles within the Development, Information Resources, and Lodging areas. In these roles, Defendant Hoffmeister directed Marriott's process for replacing and updating its Sales and Marketing, Event Management, and Revenue Management systems. During the Class Period, Defendant Hoffmeister made public statements to the market about Marriott's operations and the Company's acquisition of Starwood.

26. Defendant Stephanie C. Linnartz ("Linnartz") is Marriott's CCO and Executive VP. Defendant Linnartz has been in her current role with the Company since March 2013 and also serves on the Board's Committee for Excellence. In her current role, Defendant Linnartz has a range of responsibilities, including sales, marketing, revenue management, consumer insights and innovation, and IT worldwide. Defendant Linnartz joined Marriott in 1997 as a financial analyst and has also worked in revenue management, sales, and marketing. Prior to assuming her current role as Marriott's CCO, Defendant Linnartz was Marriott's Chief Marketing and Commercial Officer. During the Class Period, Defendant Linnartz made public statements to the market about Marriott's operations and the Company's acquisition of Starwood.

IV. CONFIDENTIAL WITNESSES

27. The Complaint relies upon numerous former employees and consultants of Starwood and Marriott in support of Lead Plaintiff's allegations. These confidential witnesses ("CWs") are described in detail below and their allegations appear throughout the Complaint.

28. Confidential Witness 1 ("CW 1") was employed by Marriott from May 2005 to March 2018. He[1] was a Software Developer and Technical Lead at Marriott's Gaithersburg, Maryland office. CW 1 reported to End User Computing & Collaboration Technical Architect Tom Simmons, who first reported to Senior Director-Systems Engineering Randy Hughes, and then to Senior Director – Workplace Engineering Darren McMahon and Senior Director-IT Workplace & End User Technology Service Delivery Brian Dishong. Through this role in Marriott's IT department, CW 1 was primarily responsible for designing, implementing, and supporting applications and solutions for Marriott's Microsoft-based systems. CW 1 was directly involved with Marriott's due diligence investigation of Starwood prior to and during the merger process, as well as the integration of the two companies' systems.

29. Confidential Witness 2 ("CW 2") was employed by Starwood from September 2014 to December 2015. He was a Senior Global Cyber-Security Consultant at Starwood's Stamford, CT location. CW 2 reported to Director of Project Management Office, Brian McCaffrey. CW 2 was hired by Starwood to study the security of Starwood applications and provide recommendations for the rollout of a Digital Identity Access Management (IAM) system to protect Starwood's various Applications and Databases Worldwide.

30. Confidential Witness 3 ("CW 3") was employed by Starwood from August 2013 to September 2016. He was a Threat and Incident Manager at Starwood's Tustin, California office. CW 3 reported to Associate Director of Threat Data Analytics Penny Hogue, who reported to Shamla Naidoo, the former Chief Information Security Officer ("CISO") at Starwood. Through this role in Starwood's IT department, CW 3 was primarily responsible for investigating threats and breaches to Starwood's computer systems and databases.

[1] All CWs will be described and referred to in the masculine to protect their identities.

31. Confidential Witness 4 ("CW 4") was employed by Marriott from September 2008 to May 2018. He held various positions, including Technical Consultant, Performance Engineer, and Performance Architect. During his first few years with Marriott, CW 4 was located at the RIO Washingtonian Center Facility in Gaithersburg, Maryland and later moved to Marriott's corporate offices in Bethesda, Maryland. CW 4 reported to Director of System Performance Sanjay Srinivasan, who now reports to VP, Enterprise Solutions Mark Stocksdale. Through his role in Marriott's IT department as a Performance Architect, CW 4 was primarily responsible for reviewing software designs and updates and designing solutions to aid in the implementation of those new designs and updates, and much of his responsibilities included maintaining Marriott's IT systems capacity and chasing IT problems.

32. Confidential Witness 5 ("CW 5") was employed by Marriott from the start of the Class Period through early 2017. He was a part of senior leadership at Marriott and a Senior Director at Marriott's corporate headquarters in Bethesda, Maryland. CW 5 ultimately reported to Defendant Hoffmeister. Through his role in Marriott's IT department, CW 5 was primarily responsible for defining Marriott's enterprise IT strategies and multi-year implementation road maps for various core and critical systems.

33. Confidential Witness 6 ("CW 6") was employed by Marriott from February 2014 to March 2018. He was a Director, Network Services at the Company's Gaithersburg, Maryland location. CW 6 reported first to Vice President, Network Engineering and then to Vice President of Infrastructure Technology. Through his role in Marriott's IT Department, CW was primarily responsible for working on integrating Marriott's and Starwood's IT systems both during and after the Merger.

V. CONTROL PERSON ALLEGATIONS

34. Defendants Sorenson, Oberg, Val Bauduin, and Linnartz, by virtue of their senior positions at Marriott, directly participated in the management of the Company, were directly involved in day-to-day operations of the Company at the highest levels, and were privy to confidential, proprietary information concerning the Company and its business, operations, internal controls, growth, IT operations and procedures, the Merger, merger and acquisition policies and procedures, financial statements, and financial condition, as alleged herein. As set forth below, the distribution of misleading information and the failure to convey material information to the public was the result of their collective actions and inactions.

35. Defendant Sorenson signed all of Marriott's Form 10-Ks during the Class Period. Additionally, Defendant Sorenson made public statements about the Merger and Marriott's operations during the Class Period as a regular participant in Marriott's conference calls, as well as other interviews and public appearances. As President and CEO, Defendant Sorenson had control over the day-to-day operations of the Company. Defendant Sorenson is also a member of the Board and two Board committees, the Committee for Excellence and Executive Committee. In his role on the Board, Defendant Sorenson attended the 2018 Annual Board Meeting and also attended at least 75% of the Board and committee meetings he was required to attend. Marriott listed Defendant Sorenson as one of its Executive Officers in the Company's 2018 Form 10-K. As alleged herein, Defendant Sorenson made false and misleading statements to investors during the Class Period.

36. Defendant Oberg signed all of Marriott's Form 10-Ks during the Class Period. Additionally, Defendant Oberg made public statements about the Merger and Marriott's operations during the Class Period as a regular participant on Marriott's conference calls. In her role as Executive VP and CFO, Defendant Oberg had control over the Company during the Class

Period and had heightened control of the Company's statements to the market. Marriott listed Defendant Oberg as one of its Executive Officers in the Company's 2018 Form 10-K. As alleged herein, Defendant Oberg made false and misleading statements to investors during the Class Period.

37. Defendant Val Bauduin signed all of the Company's Form 10-Qs and Form 10-Ks during the Class Period. In his role as Controller and CAO, Defendant Val Bauduin had control over the Company during the Class Period and had heightened control over the content of Marriott's SEC filings. Marriott listed Defendant Val Bauduin as one of its Executive Officers in the Company's 2018 Form 10-K. As alleged herein, Defendant Val Bauduin made false and misleading statements to investors during the Class Period.

38. Defendant Linnartz made public statements about the Merger and Marriott's IT department during the Class Period as a regular participant on Marriott's conference calls. In her role as Executive VP and CCO, Defendant Linnartz had control over the Company during the Class Period. Marriott listed Defendant Linnartz as one of its Executive Officers in the Company's 2018 Form 10-K. As alleged herein, Defendant Linnartz made false and misleading statements to investors during the Class Period.

39. Defendants Sorenson, Oberg, Val Bauduin, and Linnartz were aware, or at least severely reckless in not being aware, of the deficiencies in the Merger due diligence related to the security of Starwood's guest reservation database, the deficiencies in Marriott's operations of the legacy Starwood guest reservation database, and the deficiencies in the plan to move and/or merge the legacy Starwood guest reservation database into Marriott's. Through their roles as Executive Officers and directors with the Company, the Defendants Sorenson, Oberg, Val Bauduin, and Linnartz had ample insight into and substantial control over Marriott's policies and

operations, including the Company's Merger due diligence and its core operations, such as the reservation system.

VI. SUBSTANTIVE ALLEGATIONS

A. Nature of the Business

40. Marriott is the largest hotel company in the world. Marriott currently operates its hotels and other lodging business under 30 different brands in more than 130 countries and territories worldwide. Marriott's operations are massive. It has over 2,000 properties containing more than 566,000 rooms. It also has over 4,700 franchised and licensed properties with more than 729,000 rooms. The Company has approximately a 15% share of the domestic hotel market. As part of its "asset-light" business strategy, Marriott today earns the bulk of its revenue from franchise and management fees rather than from properties the Company actually owns.

41. The hotel and lodging industry is massive. In 2017, the U.S. hotel industry alone generated more than $208 billion in revenue. In that year, the ten largest hotel chains accounted for more than $53 billion in revenue with Marriott responsible for more than $22 billion of that revenue. The hotel and lodging industry is extremely competitive. Marriott vies for guests with traditional players like Hilton, Intercontinental Hotels Group, Hyatt, and Wyndham. Additionally, companies like Airbnb and VRBO compete with the hotel chains and have caused significant disruptions in the traditional hotel industry.

1. The Importance of Customer Data to Marriott

42. Though Marriott is primarily a hotel operator, the Company is also in the data business. Marriott collects volumes of personal data from its hundreds of millions of customers through its reservation system, loyalty programs, and directly from customers at point of sale locations in hotels, like gift shops. Marriott uses this customer data to engage in extensive marketing and advertising including direct marketing to its existing customer base. In order to

effectively market its rooms and services, Marriott needs to gain access to information – like personal email addresses, and detailed demographic data. The more personal data Marriott is able to collect, the wider it can cast its net for marketing purposes, and the more revenue it can generate.

43. As a part of obtaining and retaining this customer information, Marriott has, and Starwood had, a loyalty program which customers sign up for by providing their personal information as well as their credit card information. Hotel loyalty programs allow hotel companies to store customers' personal data and payment information to facilitate easy and quick transactions. Customers can also earn points that they can redeem for free or discounted stays at hotel properties. Loyalty programs thus encourage repeat customers.

44. Additionally, Marriott maintains, and Starwood maintained, personal data on every single guest that makes a reservation and stays at one of their hotels – regardless of whether they've signed up to be a member of a loyalty program - including their names, addresses, properties where they have stayed, money they have spent at the property, and more. This information is also used to market to customers, so it too is extremely valuable to Marriott. This customer reservation data is contained in what should be a secure reservations database.

45. Customers' personal data is also used to engage with Marriott's affiliated companies, like airlines and rental car agencies, assist with revenue forecasting, and to determine whether to undertake renovations and make capital expenditures on certain properties. For example, after a customer stays at a property, Marriott might send an email asking for feedback about the experience. Marriott uses this information to continue to engage the customer with the brand and obtain important information about the properties themselves. Customers' personal data is also used to enhance a customer's stay at a property – so if a customer has a preference

for a type of room, for example, Marriott already knows this. Marriott claims to use this data to "make each and every stay personalized and extraordinary."

46. Marriott has itself acknowledged the importance of this data for the Company, stating that Marriott "leverage[s] the data" it collects, and that "data is a tremendous asset for us." As part of processing the data, Marriott has a "dedicated team of marketers review social data conversations in real-time" to identify opportunities for the Company.

47. The Company has also acknowledged the significance of this data to its investors. For example, on a March 21, 2017, conference call for Marriott's 2017 Security Analyst Meeting, Defendant Linnartz discussed the importance of guest data to Marriott's ability to conduct direct marketing and attract loyalty program members. Defendant Linnartz noted the extent of the Company's direct marketing efforts, and also discussed the importance of technology to Marriott's operations in that the Company's "data shows that at many of our brands, the mobile experience drives a nearly 4 points premium in our guest satisfaction surveys." Defendant Linnartz continued that Marriott believes that "members are willing to share a lot of information with us, a lot of data about themselves but they expect us to do something with it, right, to enhance their guest experience." Marriott also uses the data to enhance their bottom line. In addition to traditional marketing, Defendant Sorenson has even suggested that Marriott will soon use guest data to charge higher prices to certain guests if the individual data Marriott has collected suggests the Company can get away with it.

48. Analysts and news outlets have also underscored the importance of customer data to Marriott and its investors. For example, on July 25, 2016, Macquarie noted that as a result of the Merger, "[i]nvestors should also acknowledge that access to a more diverse client base will generate even more valuable customer data and should improve marketing efforts, especially

towards younger and more tech savvy groups." On November 26, 2015, shortly after the Merger was announced, Wow Siew Ying for The Strait Times, an English language daily newspaper in Singapore, noted that the Merger would "expand [Marriott's] customer database," which would lower costs. On December 1, 2015, HospitalityBiz, a trade publication, noted that Marriott would be a stronger force in the marketplace due, in part, to the "'larger guest database'" it acquired through the Merger. Additionally, on September 22, 2016, Ashlee Kieler published an article for Consumerist titled *Marriott Preparing to Battle Expedia, Priceline With New Starwood Assets*, in which she said the Merger would "allow Marriott and its brands to acquire more customer data."

2. The Data That Marriott Collects

49. According to Marriott's Online Privacy Statement posted to its website during the Class Period, and the privacy statement that was posted to Marriott's now-defunct starwoodhotels.com and spg.com domains, Marriott collected and continues to collect a myriad of personal data[2] from its guests, including:

- Name
- Gender
- Postal address
- Telephone number
- Email Address
- Credit and debit card number or other payment data
- Financial information in limited circumstances
- Language preference

[2] Marriott defines "personal data" as data that identifies a person as an individual or relates to an identifiable individual.

- Date and place of birth
- Nationality, passport, visa or other government-issued identification data
- Important dates, such as birthdays, anniversaries and special occasions
- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
- Employer details
- Travel itinerary, tour group or activity data
- Prior guest stays or interactions, goods and services purchased, special service and amenity requests
- Geolocation information
- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts
- Data about family members and companions, such as names and ages of children
- Biometric data
- Images and video and audio data
- Room Preferences
- Names and ages of children

50. Marriott collects this data through a variety of means, including:

- Online Services – when guests: (1) make a reservation; (2) purchase goods and services from the Company's websites and apps; (3) communicate or otherwise connect or interact with the Company through social media; (4) sign up for a newsletter; or (5) participate in a survey, contest, or promotional offer;
- Property Visits and Offline Interactions – when guests: (1) visit the Company's properties, (2) frequent the Company's restaurants, concierge services, health clubs, child care

services, and spas; or (3) attend promotional events that the Company hosts or in which it otherwise participates;

- Customer Care Centers - when guests: (1) make a reservation over the phone; (2) communicate with the Company via email, fax, or online chat; or (3) contact customer service;

- Owners and Franchisees – owners of Marriott branded properties that are managed and franchised by the Company provide the Company with personal data from their guests;

- Strategic Business Partners – third parties that have partnerships with Marriott provide the Company with personal data from their customers to use for direct marketing;

- Other Sources – such as: (1) public databases; (2) joint marketing partners; and (3) other third parties;

- Internet-Connected Devices – e.g., a smart home assistant may monitor your activity during your stay; and

- Physical and Mobile Location-Based Services – when guests download the Company's app, Marriott "may collect the precise physical location of your device by using satellite, cell phone tower, WiFi signals, or other technologies" when guests are in or near the Company's properties.

51. Marriott also collects data from the Department of Commerce, third party booking companies like TripAdvisor, and credit card companies.

52. Once Marriott has collected this personal and other data from the Company's guests, Marriott utilizes that data for business purposes, including:

- facilitating reservations and payments, completing reservations, and processing payments;

- sending reservation confirmations or other pre-arrival messages;

- accommodating personal preferences;

- providing guests with information about the location they are visiting and the surrounding area;

- direct marketing, such as personalized service recommendations and other promotions;
- managing the Company's loyalty program; and
- data analysis, audits, security and fraud monitoring and prevention, developing new goods and services, improving or modifying current services, identifying usage trends, and determining the effectiveness of marketing campaigns and expansion of business activities.

53. In addition to using guests' personal and other data for its own purposes, Marriott also discloses that personal information to a number of third parties. Along with a catch-all disclosure stating, that Marriott may use guests' other data "for any purpose, except where [Marriott] is not allowed under applicable law," the Company discloses guests' personal data to a number of third parties, including:

- third party advertisers;
- subsidiaries of the Company;
- the Company's owners and franchisees;
- authorized licensees;
- strategic business partners;
- service providers, e.g., website hosting, data analysis, payment processing, information technology and related infrastructure provision, marketing, and others; and
- "linked accounts," i.e., accounts that allow guests to login using their Marriott rewards number or Marriott online services login and social media accounts connected to Marriott's online services account.

3. Marriott Understood the Importance of Keeping this Valuable Data Secure

54. Marriott understood how important it was to protect its customers' data, and that protecting this data was a critical function of the Company. In each of the Company's Form 10-

Ks for years ending 2015, 2016, 2017, and 2018, Marriott stated that "the integrity and protection of customer . . . data ***is critical to us***[3] as we use such data for business decisions and to maintain operational efficiency."

55. In each of the Company's Form 10-Ks for years ending 2015, 2016, 2017, and 2018, Marriott also stated that it used "sophisticated technology and systems in [the Company's] reservation, revenue management, and property management systems" and that "[k]eeping pace with developments in technology is important for [Marriott's] competitive position." Marriott also assured the market that "the integrity and protection" of customer data was "critical" to the Company.

56. Additionally, through its newly acquired website at starwoodhotels.com, Marriott made statements to the public regarding the Company's data retention and protection policies. Marriott stated that the Company only retained customers' sensitive personal information only long enough to serve the purpose it was collected for, and that it did not "give physical possession of [customers'] personal data to unaffiliated third parties outside the Starwood system." Further, Marriott assured the public that the Company "recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures." Marriott repeatedly assured the market it had security measures in place to protect customer data. Through these statements, Marriott was misleading the market into thinking the Company was taking adequate precaution with the sensitive personal information Marriott collected.

57. Marriott is also an active member of Hospitality Technology Next Generation ("HTNG"), which is a global nonprofit that fosters relationships between technology and

[3] Emphasis is added unless otherwise indicated.

hospitality companies that is "run by and for the benefit of hospitality IT executives."[4] Going back to at least 2012, HTNG has provided technical specifications for the industry, including numerous whitepapers specific to central reservations systems. As a part of its mission, HTNG hosts the Travel Information Sharing and Analysis Center ("Travel ISAC"), formerly known as the Chief Information Security Officer Forum, which has been described as the "global travel industry's new platform for security messaging, collaboration, and partnerships."

58. According to the CIO of HTNG Patrick Dunphy, the Travel ISAC is designed to help protect guests, staff, and corporate assets by facilitating confidential communication about security threats between high level IT executives. HTNG stated the Travel ISAC fulfills its mission by: (1) sharing relevant and critical information regarding information security issues in a confidential manner; (2) coordinating responses to threats "to achieve best-in-class capabilities"; (3) developing best practices specific to the hospitality industry; and (4) engaging government agencies, including law enforcement. As an active member of HTNG and a participant in the organization's forum, Marriott was keenly aware of the cybersecurity threats facing the industry, as well as its reservation database and IT systems generally.

4. Rules and Regulations that Require Marriott to Keep Data Secure

59. As discussed in further detail below in Section VI(F), Marriott is also subject to rules and regulations that govern the maintenance, use, and security of personal and financial information.

60. As a credit card payment merchant and processor, Marriott is subject to the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is an information security standard for organizations that handle branded credit cards from the major card schemes.

[4] Marriott's Chief IT Officer, Americas, Page Petry is the Vice President of HTNG's Board of Governors.

The standard was created to increase controls around cardholder data to reduce credit card fraud. PCI DSS is a proscriptive standard that sets requirements for the manner in which companies protect, store, and transmit data. For example, companies are required to build firewalls to restrict connections between untrusted networks and the company's systems. Notably, companies are also required to prevent "unauthorized outbound traffic from the cardholder data environment to the Internet." These standards and requirements put the onus on the company to design effective data security procedures. Marriott has been subject to these requirements since 2004.

61. Marriott is also required to comply with the FTC Act. The FTC Act prohibits unfair or deceptive practices affecting commerce, and that includes a company's data security. The FTC has provided guidance in various forms for companies, essentially providing instructions on how to comply with Section 5 of the FTC Act. For example, in three separate incidents in 2008 and 2009, Wyndham was hacked. The FTC initiated an enforcement action on June 26, 2012, for violations of the FTC Act including unfair and deceptive practices. In its settlement with Wyndham Hotels Group, LLC ("Wyndham Hotels") as a result of its data breaches, the FTC provided guidance on conducting risk assessments and monitoring internal safeguards and controls, in essence providing a road map for hotel chains to assess their own cybersecurity measures. Additionally, the FTC has released a memo endorsing the National Institute of Standards and Technology Cybersecurity Framework ("NIST-CSF") because the FTC said the NIST-CSF is aligned with the FTC's own standards in enforcing the FTC Act. Generally speaking, NIST-CSF guidance provides the set of standards for recommended security controls for information systems at federal agencies, but is used worldwide at major Companies as a standard for protecting valuable information.

62. Marriott also had to comply with General Data Protection Regulation ("GDPR"), which is a European regulation requiring data protection and privacy for all individuals within the European Union ("EU") and the European Economic Area. GDPR was approved by the European Parliament in April 2016 and became effective on May 25, 2018. GDPR regulates the storage, transmission, and processing of personal information of EU residents. Marriott is subject to the GDPR because it collects data from EU residents. For the purposes of GDPR, Marriott is considered to be both a data processor and a data controller. Violations of GDPR can subject a company to a fine of up to 4% of its annual global revenue.

63. Marriott also stated that it complies with the Safe Harbor Privacy Principles. The Safe Harbor Privacy Principles were designed to assist companies in complying with EU privacy regulations that preceded GDPR. While these principles were no longer in effect, Marriott was still stating that it complied with principles that required companies to, among other things: (1) transfer data only to authorized parties; (2) take reasonable measures and precautions to secure customer data; and (3) take reasonable steps to keep data current. Additionally, Marriott has certified compliance with the EU-U.S. and Swiss-U.S. Privacy Shield frameworks. Those frameworks require companies to take reasonable and appropriate measures to protect personal data and require companies to retain personal information for no longer than is necessary.

64. Marriott has also represented that it complies with the Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission[5] (2013 Framework) (the "COSO Framework"). The COSO Framework was

[5] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control - Integrated Framework: Executive Summary, Framework and Appendices, and Illustrative Tools for Assessing Effectiveness of a System of Internal Control (3 volume set), First issued in 1992 and most recently updated in May 2013. Note: COSO Members include: American Accounting Association, American Institute of Certified Public Accountants, Financial Executive Institute, Institute of Internal Auditors, Institute of Management Accountants.

designed to help businesses establish, assess and enhance their internal control. Additionally, COSO requires companies to design controls that adequately protect customer data. COSO was designed to be broader than helping to certify the reliability of financial reporting. COSO is also designed to ensure the effectiveness and efficiency or operations, and compliance with applicable laws and regulations.

B. Marriott Seeks to Maximize Value by Merging with Hotel Giant Starwood

1. Marriott's M&A Activity Prior to Acquiring Starwood

65. Between 2012-2015, Marriott purchased several smaller hotel chains known as "tuck-in acquisitions." In these transactions, Marriott folded smaller companies into its operations to enhance the Company's business in a particular geographic area or with a certain type of clientele.

66. For example, on May 31, 2012, Marriott announced that the Company signed an agreement to acquire Gaylord Entertainment Company ("Gaylord") for approximately $210 million. Gaylord was an American company that had 4 hotels with approximately 7,800 rooms spread across the Southeast. The acquisition allowed Marriott to have a greater presence in the major event market and increased Marriott's total hotel count by a mere 0.1% and the Company's total room count by just over 1%.

67. On January 22, 2014, Marriott announced that the Company signed an agreement to acquire Protea Hospitality Holdings ("Protea") for approximately $186 million. Protea was a South African company that had 116 hotels with approximately 10,000 rooms in seven different African countries. The acquisition approximately doubled Marriott's relatively small presence in the Middle East and Africa region but only increased Marriott's total hotel count by approximately 3% and the Company's total room count by approximately 1.5%. Under the

terms of the agreement, Marriott would manage approximately half of Protea's legacy properties and franchise and lease the remaining half.

68. On January 27, 2015, Marriott announced that the Company signed an agreement to acquire Delta Hotels Limited Partnership ("Delta") for approximately $135 million. Delta was a British Columbian company that had 38 hotels with approximately 10,000 rooms in Canada. The acquisition made Marriott the largest full-service hotel company in Canada. The acquisition increased Marriott's total hotel count by only less than 1% and its total room count by only approximately 1.4%. Under the terms of the agreement, Marriott was only acquiring Delta's management and franchise businesses, as well as Delta's brand and intellectual property rather than ownership of any properties.

69. The Gaylord acquisition gave Marriott a greater presence in the major event space, the Protea acquisition approximately doubled Marriott's presence in the Middle East and Africa region, and the Delta acquisition made Marriott the largest full-service hotel company in Canada. Marriott achieved all of this while spending just over $420 million and only increasing the number of hotels under its control by fewer than 160 hotels, about 30,000 rooms, and, perhaps most importantly, without taking ownership of a single property. Marriott was able to achieve greater market penetration in niche areas while maintaining its asset-light business model.

70. Analysts viewed Marriott's ability to complete these tuck-in acquisitions as a positive for Marriott and an indicator of their ability to complete other acquisitions. For example, on May 4, 2015, RBC Capital Markets noted that, as a result of the Protea and Delta acquisitions, "Marriott ha[d] experience integrating brands." Also, on November 16, 2015, the day the Merger was announced, UBS noted that Marriott was using the tuck-in acquisitions

discussed above as a sort of benchmark by which to measure the Starwood acquisition. Additionally, an analyst report published by JP Morgan noted that Marriott cited to its recent acquisitions, "(Protea, Gaylord, etc)" as "good practice" for Marriott to complete the Starwood acquisition without harming the Company's business.

C. The Massive Starwood Acquisition

71. Marriott's share price was slumping throughout 2015, along with most of its competitors. From the end of 1Q 2015 to the end of 4Q 2015, Marriott's share price fell by approximately 16.5%, while Hyatt's fell by more than 20% and Hilton's was even worse, dropping by nearly 28%. This general trend down in the hotel industry was fueled by the emergence and dominance of two sources of pressure. First, sites such as Airbnb or VRBO, allowed individuals to book their own property reservations directly with other individuals or property managers, at houses, condominiums or other non-traditional hotel-like properties oftentimes at a lower rate than traditional hotels.[6] Second, online travel agencies, or OTAs, make agreements with traditional hotel companies to offer their rooms on those booking sites – for a fee. Marriott both competed with these sites with its direct booking, and negotiated with these sites so at least some of the Company's rooms would be available on the OTAs. These forces put downward pressure on traditional hotel systems like Marriott.

72. Analysts also recognized the potentially damaging effect that these companies could have on Marriott. In an August 12, 2015, analyst report, Barclays identified Airbnb as a "long-term threat" to the hotel industry's revenues. Barclays also discussed the fact that predicted "moderate economic growth" for 2016 would cause customers to "seek out alternative accommodations, including Airbnb." That report continued to discuss Airbnb and the fact that it

[6] Additionally, property owners that utilize sites like Airbnb are not subject to the same lodging laws as traditional hotels like Marriott, leaving them free to get creative in offering unique experiences to attract guests to their homes and apartments.

had "attracted a significant amount of attention" in 2015 and that the site's emergence "potentially lessens the ability of hotels to raise prices during certain 'compression' periods as some customers may use Airbnb instead of paying higher hotel rates." On October 26, 2015, Susquehanna Financial Group published an analyst report that discussed the fact that "lodging stocks have given up all of their earlier gains and are now down ~13% YTD." That report stated there were "fears that the U.S. lodging cycle is waning, and what little incremental demand is left will be absorbed by Airbnb."

73. Given this pressure, and while the hotel industry as a whole trended down, Marriott saw the Starwood acquisition as an opportunity to consolidate power and grow the business.

74. A big part of the Merger was the acquisition of Starwood's guest reservation database and loyalty program information. Starwood traditionally attracted a younger and richer clientele, and business travelers. Marriott hoped to harness the power of these customers and leverage the customer data it purchased from Starwood to not only gain market share, but to drive revenues up as well. But this acquisition would be nothing like the $100 million to $200 million in tuck-in acquisitions of Gaylord, Protea, or Delta. The Starwood acquisition was massive – ***valued at $13 billion***.

75. In mid-to-late July 2015 Marriott entered into a confidentiality agreement with Starwood. At a regularly-scheduled meeting held on August 6, 2015, Defendant Sorenson briefed Marriott's Board on a potential combination with Starwood. On October 26, 2015, Marriott began to conduct due diligence into the potential acquisition during multiple sessions leading up to the announcement of the Merger.

76. The parties executed the Merger Agreement on November 15, 2015, and the parties announced the deal on the morning of November 16, 2015. The transaction was structured as a Marriott takeover of Starwood and the total consideration was originally supposed to be approximately $12 billion. The parties initially agreed to a price of 0.92 shares of Marriott and $2 for every outstanding share of Starwood. As one of the closing conditions, a Marriott subsidiary was buying a Starwood subsidiary to provide Starwood's shareholders with an additional $7.80 per share in compensation. However, the total compensation paid by Marriott increased to $13 billion before the closing of the Merger, as well as the amount of cash Marriott would have to pay as a part of that compensation.

77. On March 14, 2016, Starwood announced it received a non-binding proposal from a Chinese consortium led by Anbang Insurance Group ("Anbang"). The offer was all-cash and valued Starwood's shares at $76/share and the subsidiary's shares at $5.50/share for a total offer of $81.50/share. At this time, Marriott's nearly all-stock offer was worth only $69.24/share. However, by March 30, 2016, Anbang had withdrawn its offer and the deal with Marriott continued to proceed.

78. The Merger was supposed to take six to eight months to complete (closing in mid-2016) but was also subject to various regulatory approvals before the deal could be completed.

1. Analyst and Market Reaction to the Deal Underscores the Importance of the Acquisition of Starwood Customer Data to Marriott's Business

79. Analysts were excited about the deal and the effect it would have in making Marriott the top hotel company in the industry. Analysts commenting on the deal described the deal as "growth oriented" for Marriott and commented on the scale of the acquisition. For example, on November 16, 2015, Jeffries said:

> The rationale is framed as being growth-oriented, combining the distribution and strengths of both businesses to create the world's

> largest hotel company, with pro- forma fee revenue of $2.7bn from 5,500 hotels and 1.1m rooms. The deal is expected to deliver at least $200m cost synergies p.a. in the second full year after closing and be earnings accretive by the second year post- merger… MAR expects to return at least as much as the $2.2bn in dividends/buybacks announced this year, in the first year post-merger.

80. A Credit Suisse analyst, while maintaining its outperform rating for Marriott, also commented on the "considerable upside" merging the two companies, stating on November 16, 2015, "We note that the aforementioned $200m consists entirely of cost reductions (mostly SG&A), and does not take into account the considerable upside from revenue synergies associated with increased scale."

81. Credit Suisse also touted the positive nature of the acquisition by stating on November 18, 2015:

> We believe MAR will be able to unlock ***significant value*** from the acquisition, leveraging increased economies of scale, as well as an opportunity to redefine some brand aspects across the chain scale. To this point, we believe there is upside to the $200m synergy target, which consists entirely of cost reductions, and does not take into account the considerable upside potential from revenue synergies associated with increased scale.

82. The same Credit Suisse analyst stated:

> Lifestyle Powerhouse: The integration of the W brand alongside MAR's broad range of brands in lifestyle should boost its presence in this category. While growth of the Edition has been gradual, we believe the brand power and growing international distribution of the W will be significant to accelerate MAR's market share. Recently, MAR has invested in building its presence among millennials and we believe the integration of the W will help to solidify its relevance.

83. The same Credit Suisse analyst said that the Merger would help leverage the brand against companies like Airbnb that were seeking to take market share from Marriott:

> Increased Leverage with OTAs: Given the company's enhanced scale with 1.1m rooms and 75m combined loyalty program members; we see the HOT transaction as a strong offset to market concerns around positioning versus the OTA's and Airbnb's continued emergence. Further, this industry consolidation should give the company strong pricing leverage with other OTA's, as they cannot afford to lose this platform. . . . ***There is no disputing that a combined MAR/HOT entity will create a strong #1 player in the industry.***

84. On November 18, 2015, an analyst for JP Morgan noted that a "big question" still revolved around the loyalty programs and the websites of the two companies, and that Marriott had "reiterated the importance of and sensitivities around the two [loyalty] programs." A Macquarie analyst on February 18, 2016, observed: "The two companies together would form a global lodging powerhouse with more rooms than anyone else in the world." On March 3, 2016, an analyst with RBC commented that "MAR's robust select service offering and HOT's loyal members ***should drive immediate value creation***." That report also noted that "technology and marketing costs are major areas where synergies can be found."

85. Analysts also specifically commented on the value that purchasing Starwood's customer data would bring to the table, emphasizing the importance of this data in the acquisition. According to Bloomberg, Marriott's "aim was to have a bigger company that could compete with Google, Amazon and other online firms that use their knowledge of consumer preferences to gain primacy with customers." On April 4, 2016, an analyst for Susquehanna Financial Group noted that Marriott would be able to raise its revenues, "which is an example of the merits of a more powerful loyalty program post the merger." That report said, "We believe the revenue and cost synergies as cited by management are real." The report continued: "***A major strategic consideration of the deal is revenue upside from loyalty programs. Combining the SPG and Marriott Rewards programs will broaden MAR's and***

HOT's distribution and capture more share of wallet from their customers." On this point, Macquarie stated on July 25, 2016, "The merger allows Marriott to increase brand loyalty amongst its Baby Boomer Road Warriors and grow its database of affluent Gen Y and Asian customers." Macquarie also emphasized the importance to investors, stating:

> Investors should also acknowledge that access to a more diverse client base will generate even more valuable customer data and should improve marketing efforts, especially towards younger and more tech savvy groups. We also see combined marketing and sales strategies as being a strong advantage over OTAs and other hotels. With a larger marketing budget, MAR can attract a wider range of customers to join its loyalty program and to book directly from its website.

RBC echoed this sentiment on September 26, 2016 stating **"The rewards program is a high priority. In addition to scale, the SPG member base was viewed as a key benefit of the merger for MAR."**

86. After the close of the Merger in September 2016, analysts continued to discuss Marriott's competitive advantage resulting from the Merger. On November 9, 2016, Susquehanna Financial Group published an analyst report that noted Marriott "expect[s] to see savings on OTA contracts in '17 simply by applying Marriott's more favorable contract terms to Starwood hotels even assuming no change in OTA usage, and more to come in 2018." On November 10, 2016, an analyst report from SunTrust Robinson Humphrey noted that, as a result of the Merger, Marriott "will soon be able to negotiate better OTA contracts." Further, on May 16, 2017, Susquehanna Financial Group published an analyst report, which stated that "lower OTA fees should foster support for additional 3rd party financed (and developed) unit growth."

2. Marriott Conducts Inadequate Due Diligence at the Time of the Merger and Fails to Detect Numerous Vulnerabilities In Starwood's System – Including a Massive Data Breach

87. As part of the Merger, Marriott was required to conduct due diligence into Starwood to determine if Starwood was an appropriate acquisition. Defendants repeatedly said that a primary driver of the Merger was accessing the data contained in Starwood's reservation database, and joining both loyalty programs so that Marriott would be able to capitalize on the customer data it was acquiring from Starwood in the Merger. Additionally, once the Merger was completed Marriott would own all that data and technological infrastructure from Starwood as its own and be responsible for safeguarding it. As detailed in the Merger Agreement, through a series of transactions, Marriott essentially subsumed all of Starwood and its operations. This included their computer systems, reservation software and database, as well as all the personal information contained in that database.

88. It was a vital part of the Merger that Marriott perform adequate due diligence by investigating and examining Starwood's internal systems, including its reservation system, and more broadly, making sure that the assets – both physical and technological – that Marriott was purchasing from Starwood were intact and secure. This was important to investors, because Marriott was spending so much money on the transformative acquisition, and investors needed to be comfortable that what Marriott was purchasing was both worth the price, and that it would not add any unnecessary risk or liabilities to the Company. Thus, the due diligence process into Starwood's technology was expected, as technology is typically a major focus of M&A due diligence and cybersecurity is a major consideration in technology due diligence. And, the due diligence here would have to be massive and extensive – to match the breadth of the acquisition itself.

a. Marriott's Assurances to the Market

89. At the time the Merger was announced, Marriott had already conducted several weeks of due diligence. Between the time the Merger was announced on November 16, 2015 and the Merger closing on September 23, 2016, Defendants repeatedly informed the market they had conducted further due diligence, and touted their efforts in conducting "extensive" due diligence and working on the successful integration of the two companies. They also repeatedly assured investors that Marriott's prior merger experience primed them to execute the Merger successfully as well.

90. For example, on the date the Merger was announced, November 16, 2015, Defendant Sorenson filed a letter to investors with the Prospectus. In that letter, Defendant Sorenson stated: "***we don't anticipate the integration having an impact at the hotel level worldwide."***

91. On January 27, 2016, Marriott further reassured investors that the due diligence process was going well, with no issues to report, and that it was smooth sailing: "Taking into account Starwood's publicly filed information ***and the results of Marriott's due diligence review of Starwood***, the prospects for the combined company are favorable." Just three months after announcing the Merger, on the February 18, 2016, Q4 2015 Earnings Call (and with three additional months of due diligence under his belt), Defendant Sorensen said "And we are doing everything we can to plan for integration of systems and integration of business units between now and when we close so that we can implement those as quickly as possible. ***And we're optimistic at this point that this will go well.***"

92. In the 2015 Form 10-K filed on February 18, 2016 (during the midst of the due diligence process), Marriott acknowledged that "the integrity and protection of customer, employee, and company data is critical to us" and Marriott's customers "***also have a high***

expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information." Additionally, Marriott assured the market that the Company used "sophisticated technology and systems in [the Company's] reservation, revenue management, and property management systems."

93. On March 21, 2016, during a conference call to discuss the Merger, Defendant Oberg described the "extensive due diligence" that Marriott continued to conduct and stated: "We have been working intensely since we announced this deal in November to prepare for integration and of course, to understand each other's organizations and structures and start to think about how to meld those into one organization." On that same call, Defendant Oberg told investors that Marriott "had extensive due diligence" and was "spending a lot of time with the Starwood team and joint integration planning." Also during that conference call, Defendant Sorenson informed the market that since Marriott began its due diligence in October 2015: "In the further diligence we have completed in last five months, we have become even more convinced of the tremendous opportunity presented by this merger."

94. On March 21, 2016, Defendant Sorenson shared a LinkedIn Post stating "Since we announced the merger in November 2015, our integration teams have met on average multiple times a week across disciplines. ***As a result of our extensive due diligence and joint integration planning, we are now even more confident in the potential of cost savings of this transaction."***

95. During the same conference call, approximately seven months prior to the close of the Merger, to discuss Marriott's updated acquisition bid, Defendant Oberg stated, "I think one of the benefits of our time with Starwood over the past four months is being able to, continent by continent, discipline by discipline, go through and look at the way that they are

structured and the way that we are structured, to look at how responsibilities are going to be carried forward."

96. On April 1, 2016, Defendant Sorenson said that in the four months since the Merger was announced, Starwood and Marriott integration teams had met approximately 150 times, "where they are getting to know the organizations." On June 8, 2016, Defendant Oberg said that as part of Marriott's due diligence process, the Company had identified "little things about how you manage the different disciplines on the IT side in a certain geographic area."

97. Over the course of the next several months, Defendants continued to reiterate the ***"extensive due diligence" and "joint integration planning" with Starwood*** and the "***exhaustive planning***" surrounding the Merger and integration process.

98. In short, Defendants conveyed to the market during that time at least three important facts: (1) they understood the importance of securing the customer data they were purchasing; (2) they were working hard to comprehensively evaluate Starwood's systems; and (3) that there were no issues identified that would impede the Merger or the successful and financially beneficial integration of the two companies. But this could not be further from the truth.

3. Unbeknownst to the Market, Starwood Was Suffering from Massive Security Vulnerabilities That Left Customer Data Unsecured, and This Data Continued to be Unsecure After Marriott Acquired Starwood

99. At the time of the Merger, Starwood's IT systems were unsecure, outdated, and inadequate for the task of maintaining data confidentiality. Starwood's systems were the frequent subject of cybersecurity breaches. The reason for these multiple breaches was simple. Starwood's IT department was not up to the task, including running an antiquated access portal for its IT applications that was in desperate need of both updating and upgrading. Starwood

refused, or could not afford, to update its Oracle application portal and continued to access its guest reservation system through a portal that was perilously unsecure.

a. Successful Cyberattacks of Starwood

100. Between 2015 and 2017, Starwood was affected by at least five different cybersecurity incidents of varying degrees of severity.

101. On November 20, 2015, just five days after Starwood signed the Agreement with Marriott, Starwood revealed that the point of sale systems at some of its hotels in North America had been infected by malware. The malware was active in Starwood's point of sale systems from November 2014 to October 2015. The malware enabled unauthorized parties to access the payment card data of some customers, including cardholder name, payment card number, security code, and expiration date.

102. On August 14, 2016, multiple news outlets reported a data breach that affected 20 hotels, some under the Starwood or Marriott brands, owned and operated by HEI Hotels & Resorts ("HEI"). The malware that infected HEI's system was active from March 1, 2015, to June 21, 2016. Reuters noted that of the 20 hotels affected by the payment breach, 12 were Starwood hotels and six were Marriott hotels. The outside experts that HEI brought in to address the attack determined that hackers might have stolen customer names, account numbers, payment card expiration dates, and verification codes.

103. In an article titled *Revealed: Marriott's 500 Million Hack Came After a String of Security Breaches* written by Thomas Brewster for Forbes, Mr. Brewster gave several examples of security breaches at Starwood. In one example of a corruption of Starwood's system, cybersecurity researcher Alex Holden revealed to Forbes that six servers hosting various starwoodhotels.com domains were controlled by Russian botnets. Another example of a

vulnerability in Starwood's IT systems is that Starwood's ServiceNow[7] cloud computing service was found to have easily guessable passwords. From the ServiceNow portal, an attacker is able to access a company's booking information, IT security controls, and financial records. Going back to 2014, Starwood had a vulnerability on the company's website. The website was infected with an SQL injection bug. That bug could have been exploited to gain access to Starwood's database. According to Forbes, vulnerabilities in Starwood's system were being advertised on the dark web at that time.

104. As a result of these incidents Marriott was aware, or was at least severely reckless in not being aware, of the need to perform heightened diligence and thoroughly test Starwood's systems during the merger process and in operating Starwood's guest reservation database. Additionally, that these incidents occurred with relative frequency during the time around the Merger was a red flag for Marriott as to the need for heightened diligence.

b. Starwood's IT Systems

105. Former employees of Starwood and Marriott confirm that Starwood's IT systems were woefully inadequate and that these deficiencies were so obvious that Marriott knew, or were extremely reckless in not discovering these deficiencies in their due diligence process.

106. CW 5, who was a Senior Director and was employed by Marriott from the start of the Class Period to early 2017 said, in reference to the Merger, "I knew all about it, I was in leadership." CW 5 said that as a part of the leadership team, he participated in various conversations during the due diligence process where concerns about Starwood's systems were outlined and discussed. CW 5 said that he attended many due diligence meetings prior to and during the sale. CW 5 said that "all the senior technical leadership participated." When asked if

[7] ServiceNow is a company that provides various IT services, including cloud computing, incident management, performance analytics, and change and release management.

Defendant Hoffmeister was involved in the due diligence process and aware of these security concerns, CW 5 that Defendant Hoffmeister was involved in some of it and that 90% was run by CTO Tagliere. CW 5 added Mr. Rosa and Ms. Memenza were also very involved, especially in setting up the firewalls and implementing various protections.

107. CW 5 said that the entire IT leadership team sat down and went through every Starwood system before the acquisition. Additionally, CW 5 said that the due diligence process was extremely detailed and ultimately the decision was made to dispose of almost all of Starwood's system with the "sole exception" being their loyalty rewards system. He explained that the decision to dispose of the majority of the systems was due to Starwood's "tech stack" being "dated" and not meshing with Marriott's systems. According to CW 5, Marriott could not dispose of Starwood's loyalty rewards system because of the "financial viability" of the points.

108. According to CW 5, "Marriott was aware of the security flaws both before, during and after the acquisition." CW 5 said that during the due diligence process, Marriott became aware of a previous hack of Starwood's systems which they were told to disregard because it was Starwood's problem but ultimately Marriott did not remediate it in a timely manner which led to the 2018 breach. He continued that Marriott's leadership team during the Merger outlined and discussed concerns related to Starwood's IT systems. CW 5 said the due diligence process was "one of the ways we found out" about the weaknesses in Starwood's system. CW 5 said that former CTO "Tagliere orchestrated due diligence, he drilled down and marshaled the resources to make a recommendation." CW 5 said that Mr. Tagliere and Mr. Rosa, the SVP for Infrastructure struggled to see eye-to-eye. CW 5 said that Mr. Rosa eventually left the company over his differences with Mr. Tagliere.

109. CW 5 said that when "Marriott said they were buying Starwood they pulled in various people to assess, and said, 'what's your recommendation, take or port?'" CW 5 said that: "As we went through revenue management, the res system, and rewards, rewards was the only system we would keep for even a short time until a new system was built to replace both." CW 5 said that Marriott planned to "compartmentalize" Starwood's weak systems in general, including their security system, and upgrade to a system like Marriott's. CW 5 said Starwood's "infrastructure was going to be migrated to Marriott." CW 5 said the rest of the systems were not salvageable and Marriott intended to scrap them. CW 5 said Marriott had a number of meetings "where we discussed, 'how will we do this?'" before realizing Marriott would have to "build new systems for both." CW 5 clarified that he was referring to either addressing or merging Starwood's loyalty rewards system.

110. CW 5 advised that Starwood's Oracle stack was beyond being patched and it would have cost hundreds of millions of dollars to fix. He explained that the stack was at capacity and could no longer be patched or expanded upon. According to CW 5, this was primary reason that Starwood was looking to be acquired and Marriott knew it. He added that he was told that Starwood's system could not add any new hotels to its systems because it had "reached its upper limits." CW 5 said that Marriott chose to then dispose of Starwood's entire system with the exception of their loyalty system which they had wanted to migrate. CW 5 went on to say that ultimately Marriott had to build a new loyalty system which is now called "Bonvoy." He added that he knew a lot about the decisions related to the loyalty system because it had an impact on the reservations system that he ran, so he was "pulled in."

111. CW 5 said that it was possible that Starwood may have withheld information about the Breach from Marriott but he did not know. CW 5 further explained that because of the

concerns about Starwood's security posture, the decision was made to keep Starwood's systems separate until they could dispose of the majority of their systems because it could not "mesh" with Marriott's." CW 5 said that the general consensus amongst Marriott leadership was that there as a high "likelihood of a threat." CW 5 added that Ms. Memenza "saw this as too much of a risk" and ultimately left Marriott because of the Starwood acquisition.

112. CW 5 clarified that he was referring to the IT leadership at Marriott who had a concern that Starwood's systems were risky so they decided to "get rid" of them. He went on to say that after reviewing Starwood's systems prior to the acquisition, it was clear that they were not as protected as Marriott's. CW 5 went on to recall attending an offsite meeting with over 100 of Marriott's leaders, where they had a "scorecard" and reviewed each system, system by system to identify and "highlighting" issues specific to that system. According to CW 5, this offsite meeting took place prior to the acquisition and they did not tell Starwood their findings.

113. CW 5 said that the biggest weaknesses that they identified with Starwood's systems were their lack of operational discipline and their lack of "checks and balances." CW 5 said that the hack that had been identified was "explained away" and they claimed that Marriott did not have "liability" for that hack since it was pre-Merger.

114. CW 5 also recounted how that Marriott's Board of Directors should have had a "heightened" sensitivity to being hacked since it was their loyalty points that were stolen in the hack. According to CW 5, around 2013/2014, there was a hack of the Board's loyalty points which was approximately $10 million in value. He reiterated that given the stature of the executives that the hack impacted, their "sensitivity of being hacked [in the future] was very high" following that hack. He added that they were also aware of the White Holdings' hack which are franchises owned by Marriott.

115. According to CW 1, a former Software Developer and Technical Lead for Marriott, Marriott's IT systems were superior to Starwood's. He also said that Marriott knew it was vulnerable as a result of the Starwood acquisition and that Starwood's IT department had "poor security hygiene." Additionally, CW 1 said that Marriott invested a lot of resources into the "tokenization process" with their customers' credit card information. He said the reason for investing heavily in the tokenization process was because Marriott knew that credit card information was a known high-value target for hackers. CW 1 also said that it was apparent to some that Starwood held back on capital investments in IT because much of Starwood's equipment was over ten years old. He continued that IT hardware is supposed to be upgraded at least every five or six years because "the attrition rate goes way up after five or six years." CW 1 said he believed that Marriott's senior executives should have seen or been aware of weaknesses in Starwood's systems since Starwood's systems were so old. He also said that he did not see how Marriott's senior executives could not have known because replacing IT hardware was a capital expenditure would have to be approved by senior management.

116. CW 1 also said that Marriott knew that "Starwood's network was understood to be vulnerable." Additionally, CW 1 said Marriott "already knew Starwood had an incursion, probably right before the acquisition." CW 1 described Starwood's network as "basically a foreign network with security problems." CW 1 said there was an internal thought that by not digging too deep into Starwood's systems Marriott could avoid finding anything. CW 1 suggested that the hope at Marriott was that any IT vulnerabilities at Starwood would "wither on the vine."

117. CW 2, who was a Senior Global Cyber-Security Consultant at Starwood from September 2014 to December 2015, said that Starwood used a very antiquated version of the

Oracle portal for its IT system, which contained over 150 applications, including the Starwood's Reservation and SPG Loyalty Points systems. CW 2 explained that Starwood refused to pay Oracle for maintenance support for years - so "nothing was updated or patches implemented to prevent hacking." CW 2 said this left Starwood's Oracle portal seven years past its end of life and very vulnerable to attack by hackers. CW 2 described the cybersecurity group/program at Starwood as a "joke" with only a five member team to support security activities for over 100,000 employees, more than 40 million customer users, more than 150 applications, and thousands of POS systems worldwide.

118. CW 2 said that Starwood utilized Symantec for its Security Information Event Management ("SIEM")[8] but CW 2 said he did not think that this was scaled up to provide proper security log monitoring for all of Starwood's more than 800 servers. CW 2 said that without someone monitoring the SIEM System 24 hours a day and seven days per week (at all times), it was ineffective to monitor hackers within Starwood's application servers and databases. CW 2 explained that there was no mention of the SIEM tool being outsourced to another managed service provider. CW 2 said he identified this weakness during his engagement with Starwood and suggested Starwood use IBM's SIEM tool. CW 2 explained that there was no privilege access management ("PAM")[9] tools present to store application and database service account credentials securely like CyberArk or BeyondTrust - none of these tools existed at Starwood to manage service accounts for login to application servers and database servers securely in a PAM

[8] According to a trade publication, in the field of computer security, security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

[9] According to trade publications, Privileged Access Management (PAM) Privileged Access Management (PAM) refers to a class of solutions that help secure, control, manage and monitor privileged access to critical assets.

vault. CW 2 explained that without proper PAM tools to manage Service accounts - this is where hackers can hack into the "root access" to the IT Applications and Database systems. CW 2 further explained the linkage of the Digital Identity Access Management ("IAM")[10] System with the PAM system for service accounts connection to Digital Identity was lacking at Starwood - since there was no PAM System there. CW 2 stated that the IT and database team mentioned that they used Jump Servers to provide access jump into applications and databases. Moreover, CW 2 said these service accounts were not stored in a PAM system securely - or managed in a secure way manually. CW 2 continued that this is where hackers first look into, and use service accounts to get into IT systems, applications, and databases. CW 2 stated that 95% of all data breaches start through this method whereby hackers gain access to service accounts.

119. CW 2 said that Starwood outsourced the development and operations of its IT Systems, reservation system, SPG Loyalty System and other system-related projects, to Accenture Consulting. CW 2 provided that Accenture had approximately 1500 to 2000 workers from India on-site at the Stamford, CT and Braintree, MA Locations, where these IT and security projects were implemented. CW 2 said that throughout his tenure with Starwood, Accenture knew of Starwood's IT security vulnerabilities.

120. CW 2 said that Starwood was conducting business with all their customer user and employee user IDs and passwords stored in the Starwood databases "in the free and clear" and "all their passwords were not encrypted at all." CW 2 said this "lack of encryption existed for quite some time (years) before he started in 2014 and involved all their strategic digital

[10] According to trade publications, identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. With an IAM framework in place, information technology (IT) managers can control user access to critical information within their organizations.

assets" and referred to Starwood's systems as "wide open." CW 2 said that Starwood had exposed all their strategic digital assets because all of their passwords were "in the free and clear" with no attempt at encryption until 2015. CW 2 described these digital assets as "Swiss cheese" because of all the open security holes and vulnerabilities for hackers to access. CW 2 explained that Starwood had over 150 mission critical applications, including the reservation system and the SPG Loyalty System, that were wide open and plugged into the seven year past end of life Oracle portal software - this was learned from Glenn Mannke[11] of Braintree, MA. CW 2 said that Glenn always had issues keeping the Oracle portal up and running - and getting Oracle support because of the end of life issue and Starwood not paying for Maintenance Support while CW 2 was at Starwood.

121. CW 2 said that as a result of his system assessment, he told Starwood "to implement an Identity Access Management (IAM) system to secure their Applications and Databases and PAM Service Accounts." CW 2 said that Starwood knew they had serious vulnerabilities but did not "want to spend $10-$20 million on a system rollout." CW 2 said that instead, Starwood "went on the cheap" and directed CW 2 to implement a program he referred to as "salted hash." CW 2 described "salted hash" as a "quick" and "dirty" fix for encrypting the user passwords that were stored "in the free and clear" in the Starwood databases. According to CW 2, the best that "salted hash" encryption could hope for was to slow down, rather than stop, attackers and hackers from gaining access to these passwords. CW 2 stated that the Starwood database architects knew the "salted hash" algorithm could be hacked eventually on the user passwords in the database.

[11] According to a publicly available database, Glenn Mannke was a Director with Starwood beginning in 2001 and is currently employed with Marriott as a Senior Director Identity and Access Management.

122. CW 2 said he reported these serious results of his assessment to upper management, including Starwood's then-CIO Martha Poulter, and other Starwood executives (Pat Foley, Brad Carr, Sandy Bourgone, Glenn Mannke, Kevin McCaffrey). CW 2 said "upper management would rather discuss it than do what was necessary." CW 2 said that rather than address the issues in a meaningful way, Starwood settled for a quick solution to try and secure their top digital assets. CW 2 said this quick fix was not significant enough to address all the issues he found in 2014 and 2015. CW 2 attributed the vulnerabilities in the system and lack of remediation to Starwood's thrifty approach towards cybersecurity. CW 2 said that Starwood's applications were built without IT security in mind.

123. CW 2 said he worked closely with three Starwood executives, Shamla Naidoo,[12] Glenn Mannke, Kevin McCaffrey,[13] Brad Carr,[14] and Pat Foley[15]. CW 2 said Mr. Foley, who was a Director of IT Security at Starwood, knew of the serious nature of the neglected system for a number of years prior to CW 2 starting with Starwood, but Mr. Foley did nothing about it (despite his experience working as an expert in IAM for Fidelity) for Foley's eight years there before CW 2 arrived. CW 2 said he brought suggestions for security issues related to external consumers and explained they should be part of the IAM system rollout - but Mr. Foley replied;

[12] Shamla Naidoo is the Global Chief Information Security Officer of IBM. Prior to joining IBM, Shamla was Vice President of Information Risk and Security at Starwood Hotels and Resorts. Previous roles include Chief Information Officer, Chief Information Security Officer and Chief Risk Officer at leading companies including WellPoint, Northern Trust and ABN AMRO.

[13] Kevin McCaffrey according to his LinkedIn profile dated, December 14, 2018, is presently employed by Marriott International as Director Program Management. He was Senior Project Manager at Starwood from November 2011-February 2014.

[14] K. Bradford Carr according to his LinkedIn profile dated, December 14, 2018, was employed for (18 years) at Starwood Hotels until December 2017. He was last positioned as VP, Enterprise Systems and held other executive titles. He is presently listed as Strategic Account Director at Amadeus IT Group since March 2018.

[15] Pat Foley according to his LinkedIn profile dated, December 14, 2018, was employed at Marriott International as VP, IT Security-Risk & Compliance from October 2016-January 2018. Prior, he held positions at Starwood Hotels & Resorts from August 2007. He is presently listed as being employed at Manulife as AVP-Global Infrastructure Services Information Risk Officer.

"'No! Don't even touch external customer IDs.'" - which resulted in keeping the external Customer Access perimeter totally unprotected and unsecure for more than 40 million customer users that accessed Starwood systems.

124. CW 2 said the vulnerabilities in Starwood's system left both internal employees and customer information exposed. CW 2 said that Starwood's executives were aware of the hackers in Starwood's PoS system[16] and a hack of SPG Loyalty System[17] as well. CW 2 said that Starwood was particularly sensitive to data security at this time because of the breaches at Target, Home Depot, and others. CW 2 also said the vulnerabilities led to certain of Starwood's own executives having their SPG accounts hacked a couple times while the CW 2 was at Starwood. He stated that the initial goal after his hiring was for him to try to secure the applications.

125. CW 2 also said that Starwood had "evidence of unauthorized" access to their systems since July 2014 because they lacked proper SIEM log monitoring for all Starwood applications and databases. CW 2 summed up Starwood' s cybersecurity issues by stating, "they were post end of life on the entire product line and all their apps were wide open" and "there was no IAM security to keep people out." CW 2 suggested that when Starwood's Point-Of-Sale system was hacked, it's possible that the hackers could have dropped Malware into their portal.

126. CW 2 said when he started at Starwood, the IT security staff was only about five people and only one of them might have held a Security CISSP certification. CW 2 said this was an extremely small team and insufficient to protect against vulnerabilities and incidents; and there was no IAM Support, and 24 x 7 SIEM log monitoring- as there should have been for a worldwide company like Starwood. CW 2 stated there was no mention of GDPR certification

[16] Referring to the publicly announced point of sale hack described in ¶ 101.

[17] Referring to the SPG loyalty program.

support or considerations for Starwood's security operation in European countries while they were operating worldwide.

127. CW 4, who worked as a Technical Consultant, Performance Engineer, and Performance Architect for Marriott from prior to the Class Period to May 2018, said that hacking methods and techniques for an open system like Starwood's Oracle database were "far more widespread." CW 4 believed that Starwood's Oracle database ran on Linux, and described such open systems as a bigger target for hackers. CW 4 also said that that Starwood appeared on most IT personnel's radar in 2016. CW 4 said that he believed Marriott's IT security personnel was somewhat understaffed, especially after Senior VP, Information Protection and IT Security, Kathy Memenza, left the Company. He recalled that with Ms. Memenza's departure, Marriott came to rely on consultants for their IT security projects.

128. CW 5 said that Starwood had a contract with Accenture, who managed Starwood's infrastructure and security. CW 5 said that the life of Starwood's reservation system could not be extended because Starwood had not properly invested in the system and could not afford to upgrade it. CW 5 said the fact that Starwood was "constrained by picking the wrong technology stack" was the primary reason for Starwood's sale, and referred to Starwood's Oracle stack as a "dead end." CW 5 said that eight years prior to the Merger, Starwood made a poor investment in its technology that locked it in a tough cycle. CW 5 said that Starwood chose the wrong technology path and could not expand their reservation system. CW 5 said that after Marriott assessed Starwood's reservation system, "it was clear it was going to be a migration, not a merge." CW 5 said that Marriott wanted to "isolate any problems Starwood had."

129. As a result of these deficiencies and other issues, Starwood was often the target of cyberattacks and was frequently unable to protect its customers' sensitive, personal information and succumbed to many of the attempted intrusions of its systems.

130. In fact, ***at the time of the Merger Starwood's system had already been breached***. Stretching back to at least July 28, 2014, Starwood had a breach in their guest reservation database that allowed attackers to steal the sensitive personal information of more than 380 million guests. The names, addresses, payment card information, passport numbers, and other sensitive data were compiled into tables and stolen on at least two different occasions, once in 2015 and again in 2016. The attackers were able to aggregate the data on hundreds of millions of guests, archive that data, prepare it to be sent, connect to outside, malicious IP addresses, and export files, all while Marriott was allegedly conducting "extensive due diligence." However, despite supposedly conducting "extensive due diligence" over the course of approximately a year, Marriott failed to detect the Breach, and would fail to detect it for another 2 years.

131. More importantly, Marriott either failed to discover the obvious deficiencies with the Starwood system described above which exposed the customer data it would now own, or was severely reckless in not detecting these glaring and obvious deficiencies and they are liable for misleading the market as to the extent of its due diligence and, the positive progress of the integration. Marriott is also liable for failing to safeguard this important customer data (while simultaneously touting the importance of safeguarding the data), and for omitting information to the market about the terrible and risky state of the assets it was purchasing for $13 billion.

4. Marriott Ignored Significant Red Flags Surrounding Starwood and the Merger

132. Marriott knew about or recklessly failed to discover the gross deficiencies in Starwood system that former employees of both companies describe above. In addition to

having access to the obvious information provided by former employees in the course of their due diligence process, Defendants also disregarded numerous red flags that existed at the time of the Merger. These red flags should have (but didn't) put Marriott on heightened notice that they needed to exercise particular care in reviewing Starwood's systems, and if they discovered any kind of vulnerability, to immediately remedy the vulnerability to protect their customers data.

133. In the years prior to the Merger signing, Marriott was aware of at least ***nine*** data breaches in the hotel industry alone. On March 5, 2015, approximately seven months before Marriott began its due diligence for the Merger, Mandarin Oriental Hotel Group ("Mandarin Hotels") announced a breach of its credit card systems in which the credit and debit card information of thousands of guests was stolen. Also, on November 24, 2015, just over a week after Marriott and Starwood signed the Merger Agreement and Marriott began its more involved due diligence, Hilton Worldwide Holdings Inc. ("Hilton Hotels") announced two breaches, one of which was very similar to the breach of Starwood's reservation database in that 360,000 customer records were aggregated for removal. Less than a month later, on December 23, 2015, Hyatt Hotels Corp. ("Hyatt Hotels") announced that its customers were subject to a data breach through malware the company discovered on its payment processing systems at various properties, including front desks. One report published on December 24, 2015 by United Press International on the Hyatt Hotels breach noted that in 2015, across all industries, more than 178 million records had been affected by 766 data breaches.

134. Additionally, the Merger Agreement was signed less than two years after Target reported a data breach affecting more than 40 million customers. Also in that time period, Yahoo announced the largest data breach in history to date. The day before the Merger was closed, Yahoo announced a breach of approximately 300 million records. Less than three

months later, Yahoo corrected that number and informed the public the breach actually affected every single one of Yahoo's customer records, a total of approximately 3 billion. Further, in the approximately ten months between the signing and the closing, an additional six breaches were announced in the hotel industry alone.

135. Even a cursory review of Starwood's IT systems would have revealed the glaring difference between the state of Starwood's poor systems and Marriott's secure system, which is itself a red flag.

D. After the Deal Closes, Marriott Misleads the Market About the Effectiveness of the Integration Process and Fails to Safeguard its Valuable Customer Data

1. The Integration Process

136. After the Merger was completed on September 23, 2016, Marriott continued to work on integrating the Starwood system into the Marriott system to capitalize on Starwood's customer data. However, during this time, while working to integrate the two systems, Marriott continued to separately operate the legacy Starwood reservation system.

137. Defendants also continued to mislead the market about the status of the integration. For example, on February 16, 2017, during the Company's Q4 2016 earnings call, Defendant Sorenson assured the market that Marriott was "pleased with the pace of integration." Additionally, on March 21, 2017, Marriott held a conference call for the Company's 2017 Security Analyst Meeting. On that call, Defendant Linnartz discussed the "access to the legacy Starwood accounts and customer information globally" and told investors they were "still mining the data." Further, Marriott continued to tout its sophisticated technology and systems (which now also included Starwood), including those used for reservations. Despite warning of some cyber risks, Marriott failed to disclose facts that would have shed light on these risks – including

that Starwood's Oracle application portal which housed the reservations system was past end of life, could not be patched and was unsecure.

138. Indeed, former employees confirm that in addition to the poor due diligence completed at the time of the Merger, and the unacceptable condition of Starwood's systems that Marriott purchased (and failed to fix), the post-Merger integration process was both rushed, underfunded, and ineffective to remedy Starwood's myriad problems.

139. CW 1 stated he was directly involved in the integration of the two companies' systems. CW 1 continued: "The general consensus was there needed to be a way to minimize connectivity between Starwood and Marriott infrastructure." CW 1 said that as a result of this knowledge, Marriott approached the transition with a "low level of trust" with the Starwood network and connected devices. CW 1 described Starwood's network as "basically a foreign network with security problems." CW 1 said that "given the Herculean effort of trying to absorb a huge company" like Starwood, Marriott just wanted to try to keep their heads above water. CW 1 said that Marriott made the decision to purchase "ridiculously expensive" hardware that CW 1 believed was unneeded. According to CW 1, this decision was made because Marriott was overwhelmed by the size of the Starwood IT integration and unsure how to navigate it. CW 1 said that for Marriott, time was the enemy and that the initial integration of Starwood's IT systems into Marriott's was "painfully slow." CW 1 further explained that Starwood had "weird systems" and they knew that there were issues with them.

140. CW 1 said Marriott was "house poor" following the Starwood acquisition and explained that Marriott had spent so much money on the acquisition that they did not have the money to invest in resources such as products to measure and assess IT security. CW 1 recounted how frequently Marriott would need to pull resources from other teams to assist with

IT security following the Starwood acquisition. CW 1 said that another aspect of Marriott's IT that he found to be questionable from an IT security standpoint was the fact that they had Microsoft Active Directory at over 600 properties during his tenure and that he has heard that they are now up to 900 properties. CW 1 continued to recall how frequently, properties "exited [the] system" and they would need to locate where the physical server and bring it back to Marriott. CW 1 said they referred to this internally as "Operation Donkey Cart."

141. CW 1 said that the driving force behind data security at Marriott was PCI compliance. He also said that both Marriott and Starwood had used Accenture for many years before and after the acquisition. CW 1 said that Accenture was the "constant" in the equation for both companies and that Accenture was involved in every aspect of both companies' IT.

142. CW 1 said that he and his colleagues encountered a number of "red flags" during the process of converting the Starwood computers to the Marriott system. CW 1 said that the conversion process involves preparation of the server at the local level and installation of the operating system by the local IT department. CW 1 said the local IT department then connects the server to Marriott's network and Marriott's IT department checks the server remotely. CW 1 recalled one "red flag" where two hotels in Jordan used the same IT technician to set up the system. That IT technician was a "former Starwood person" who stayed on with Marriott post-acquisition. CW 1 said that the IT technician had compromised the system prior to connecting it to Marriott's system. CW 1 said that same IT technician did the same thing two weeks later at a different location.

143. CW 1 also said that he did not recall any formal or official roadmap for the integration, and stated "the whole thing was so fluid." According to CW 1, as a part of the integration Marriott had to "re-image" all of Starwood's desktop computers, including those

computers at the front desks of Starwood's hotels and those computers processing Starwood's reservations. CW 1 stated that a significant part of the integration process "was all the work pre-staging" the computers for the reimaging. According to CW 1, Marriott's "general approach on a technology level is you go into the hotel, all the computers are re-imaged, we put our Marriott system on them, and create user accounts for the associates to log into."

144. CW 1 added that he did not believe anyone at Marriott appreciated how long a proper integration would take, considering that Starwood had around 1,500 properties selected for the integration worldwide. CW 1 went on to compare the Starwood integration to Marriott's previous integration of a hotel chain in Canada's systems, with only 25 locations, that took 2 years to complete. According to CW 1, only a few individual Starwood properties were completed by the time his tenure ended in March 2018. CW 1 also said that Marriott did not appreciate how long the integration would take and said the real timeline would be much longer than the 2 years it took to integrate Delta. CW 1 explained that he had previously been involved with the Delta and Gaylord mergers which involved significantly less properties and those were debacles on the IT integration, "we needed NASA."

145. CW 1 said that, as to the Merger, "Marriott wanted to do all this crazy stuff." CW 1 said that as a result of the Merger, Marriott was "going to absorb 1500 hotels, some they were going to spin off due to saturated markets, but they didn't want to spend additional money." CW 1 said that Marriott could have done more to ensure a safer transition between the systems after the Merger. CW 1 compared the variety of security challenges faced by hotel companies to the "wild west."

146. CW 1 said that Marriott was not eager to spend too much money facilitating the integration of the two companies, considering the price the Company paid for the acquisition.

CW 1 said that Marriott's lack of spending and resources on IT security may be why the integration took so long, and why the Company did not pick up the Starwood breach sooner. He added that endpoint security is expensive. According to CW 1, the threats caused by a new breed of bad actors, including state-sponsored hackers, has led endpoint security to being expensive. He continued that 99% of the IT decisions at Marriott came down to financial expense consideration. As a general example to illustrate his point, CW 1 said that an IT security measure that cost $1 per computer to implement would be approved while that same measure would be denied if it cost $2 per computer. CW 1 also said that in every meeting he attended there was always discussion of figuring out how to get things done in IT without spending additional money.

147. CW 1 said that a lot of major IT purchasing decisions at Marriott were made higher up the chain of command and described senior management as "kind of stingy." CW 1 said that senior management would often reject proposals for IT spending outright, without entertaining the proposal. CW 1 also stated that Marriott wanted to do the Merger without spending the money necessary to do it right. He went on to say that adding to the expenditures, difficulty, and time consumption involved in the Marriott-Starwood IT merger was that Starwood has properties in every country, making such mergers "murky" when accounting for the policies and governance from country to country. CW 1 described the current challenges faced in IT security as "the Wild West," and said that it would be fair to say that Marriott "could have done more." CW 1 added that the threat capability generally has "gone way up" and that end-point detection is not as an effective method as it once was. He described the attitude towards IT security at Marriott as one in which the motivation for management to upgrade after a breach rather than proactive security measures.

148. CW 1 said that the entire IT organization was run by Defendant Hoffmeister throughout the Class Period. CW 1 said that Defendant Hoffmeister's reporting chain changed, that at one point it was Defendant Sorenson but that he may have reported to another executive, but that Defendant Hoffmeister sat on the sixth floor with Defendant Sorenson. CW 1 recalled attending many Town Hall meetings where Defendant Hoffmeister would say "I'm not an IT guy" and that he spent years in finance. CW 1 also said that the sentiment following the acquisition at the Town Hall meetings was uncertainty and concern over the extent of work it would take to integrate such a large acquisition given their experiences with significantly smaller acquisitions.

149. CW 1 explained that Marriott had traditionally performed two different audits of their IT systems annually, one focused on PCI compliance and the other focused on System Organizational Controls driven by SOX. CW 1 also said that in March 2016, he attended a presentation about a third, unexpected audit that was conducted. He found out at that presentation that the third audit had been commissioned by the Board of Director's Audit Committee. He advised that this third audit was similar to the other two audits in that PWC, the auditors, collected random samplings of data and did their own discovery work. According to CW 1, vulnerabilities with Marriott's business IT systems including exposure to the internet and issues related to the guest system were identified by this third audit and presented in March 2016. CW 1 said that everyone was aware of the findings from the third audit, including the Board of Directors, Defendant Sorensen and Defendant Hoffmeister. CW 1 added that they also knew that Starwood's IT system was even worse. CW 1 advised that the PWC auditors were checking for vulnerabilities in Marriott's system and that they attached all different aspects of the systems to perform this audit.

150. According to CW 3, who was a Threat and Incident Manager at Starwood's Tustin, California office from August 2013 to September 2016, "a lot of knowledge on the Starwood network side left," which meant Marriott "lost a lot of subject matter expertise prior to and shortly after the Merger."

151. CW 3 said he learned from former colleagues who remained at the company after he left that, after the acquisition, Marriott treated Starwood's network as less of a priority than Starwood did prior to the Merger. CW 3 stated: "Starwood's network was a little forgotten about." CW 3 said he had discussions with Marriott's acquisition team regarding network security prior to the acquisition being completed. CW 3 said he decided to leave Starwood after the Merger because he did not like the direction the IT department was headed. CW 3 described Starwood's network security team as a "lift and shift" after the acquisition. CW 3 said that Starwood's network security team was told they would be terminated one year after the Merger. He said this lack of job security caused many Starwood employees with knowledge of Starwood's network to leave. CW 3 said that "a lot of knowledge on the Starwood network side left" and that Marriott "lost a lot of subject matter expertise prior to and shortly after the Merger."

152. CW 4 said that during an acquisition by Marriott, there was "typically an audit" based on the "particular security standard" that the newly acquired company used. CW 4 stated there were established procedures for auditors to follow to verify that required controls were in place. CW 4 said that these were standard practices at Marriott, and that the Company had an established set of procedures set in place by Ms. Memenza's IT Security team. CW 4 stated that Marriott maintained its main customer database on a mainframe-based system but that Starwood was not as up-to-date with modern security best practices. CW 4 said that a "mainframe system

will typically have fewer hacks, so it was a bit more secure than Starwood's Oracle database running on an open system." CW 4 said that hacking methods and techniques for an open system like Starwood's Oracle database were "far more widespread."

153. According to CW 6, a former Director, Network Services for Marriott, after the Merger it "quickly became apparent" that Marriott's existing systems could not handle the integration. He added that the project was a "whole big convergence" and required what was essentially "a complete infrastructure overhaul" for Marriott and that the integration project was a "full data center rebuild." CW 6 said that Marriott either did not forecast the costs of the integration or the cost was "a lot bigger" than they anticipated. He said that in planning for the Merger and integration, nobody was thinking past day one but that shortly after the closing of the Merger, the "reality of the magnitude started to hit us." CW 6 also said that the Merger was unique and very difficult, given the size of the two companies and said that Starwood's IT systems and security were not up to Marriott's standards. He added that during the Merger process, Starwood admitted to Marriott that Starwood's IT security was inferior to Marriott's.

154. CW 6 said that Marriott originally treated Starwood as a very large vendor that had systems that needed to be firewalled and kept separate until those systems met Marriott's standards. CW 6 stated that the project to integrate the IT systems of Starwood into Marriott's was called Project Solar, and that he was involved with it from the very beginning. CW 6 said that Project Solar was initially planned in three phases. He stated that Phase One consisted of creating Virtual Private Network ("VPN") tunnels, which CW 6 said were low cost, encrypted connections that allowed individuals to send information from Starwood's primary data center in Arizona to Marriott's primary data center in Gaithersburg, MD. CW 6 said with VPN tunnels "you get what you pay for" and there was some latency in the data transfer. CW 6 also noted

that Phase One was a "stop and go project" and that the connection between Marriott and Starwood had to be shut down and reopened each time Anbang became the leading bidder over Marriott in March or April 2016.

155. CW 6 said that Phase Two was about building circuits between the data centers and controlling the bandwidth that was needed, which included building up the bandwidth to handle the amount of data that would be transferring between the two companies' IT systems. He said that Marriott decided to forego a more secure option for the circuits because of the high price and went with the lower cost, less secure option. CW 6 also stated that Marriott wound up having to spend significantly more money on boosting the bandwidth because of the large amount of data coming from Starwood.

156. CW 6 said that Phase Three involved eventually connecting the Starwood properties after being properly firewalled. CW 6 said that in contrast to the original plan for Phase Three, all but a few of Starwood's properties wound up being connected to Marriott's system without being firewalled. CW 6 said the data centers were firewalled, but the Starwood properties were not. He said the original plan would require Marriott to "build a global network of firewalls." CW 6 continued that a compromise was made at the property level and Starwood's properties were brought in to Marriott's system without firewalls. He said the process of integrating the properties without firewalls was still ongoing when he left Marriott.

157. CW 6 said he believed there were two reasons for the changes to the original plans for Project Solar. First, he said there was a "cultural change" within Marriott's IT Department, starting around the time of the announcement of the acquisition. Second, Marriott significantly underestimated the amount of money and resources it would take to properly combine the IT systems of two very large corporations, each with a global presence. CW 6 said

that regarding the cultural change, the three original principal Marriott leaders of Project Solar were all gone shortly after the close of the Merger either on their own or because their job responsibilities were made redundant when Starwood staff joined.[18] CW 6 described these changes as "a VP run off shortly after the close" of the Merger and there was "a huge influx of people from Disney and NBC." CW 6 said he believed that Marriott's priorities and focus moved away from security with the change in IT leadership during the acquisition and integration process. In addition to the departure of the three principal leaders, Senior VP – Information Protection IT Security Kathy Memenza left in the summer of 2016 and another key leader in the IT Department, Director of Infrastructure Security Dale Lindsay left in early 2018. CW 6 said that Ms. Memenza and Mr. Lindsay were two of Marriott's key people with IT security oversight and that the Company's "whole direction changed" after Ms. Memenza's departure in the summer of 2016.

158. CW 6 said that the plans for Project Solar changed with the new leadership and that, from his perspective, planning was not as diligent under the new leadership structure compared to Marriott's previous and usual standards, and that there was not as much focus on IT security. To illustrate this change, CW 6 contrasted the approaches of Mr. Blanchard, who prioritized getting a system to work before using it, and Mr. Rosa, who focused more on scale. CW 6 described the integration process after the change in leadership as "more chaotic," "time slowed" in reference to projects falling behind, and that the integration process was a lot bigger

[18] CW 6 said that Senior Vice President of Global Information Resources - IT Delivery Hank Weigle, who reported to Defendant Hoffmeister, left after the announcement of the merger, Senior Vice President – IT Infrastructure Daniel Blanchard left during the integration process, and Vice President – IT Network Engineering & Operations Bob Galovic, CW 6's initial direct report, left shortly after the close of the merger. CW 6 said that Mr. Weigle was replaced by Senior Vice President Technology Delivery and Operations Alan Rosa, who also reported to Defendant Hoffmeister, Blanchard was replaced by Global Vice President of Infrastructure Engineering & Operations Lenny Guardino, and Mr. Galovic was replaced by Jim Tietjin.

and more expensive than they originally planned for. He said the new leadership in Marriott's IT Department wanted the "biggest, baddest, fastest" systems and expected employees to "build it yesterday." CW 6 said that Marriott's new management "wanted to build an empire."

159. As an example of the shift away from diligent IT security processes that Marriott previously followed, CW 6 detailed Marriott's failure to establish Network Access Governance ("NAG") for Project Solar. CW 6 said that he was tasked with creating the NAG plan, which included planning for the establishment of a Board of Governance for the project, identifying what security applications and networks would be required, what the pass/fail standard would look like regarding the testing of Starwood's IT systems, and how to vet IT security, as some examples. CW 6 said that this plan was never implemented and that if it was replaced by another, he was not aware.

160. As to the unexpected cost increases related to the Merger, CW 6 reiterated that the IT merger process was a lot bigger and more expensive than what was originally anticipated. CW 6 said that it became apparent by the end of 2016 or early 2017 timeframe, and that is when management running the IT merger process were "starting to ask for more and more money." CW 6 noted that Marriott management's primary focus was getting the loyalty programs integrated in time for the closing of the Merger, which was completed on time, but that other "huge projects" were running late and had to "be done yesterday." CW 6 said that he knew about the increased costs because he was responsible for preparing the budgets for much of the work on Project Solar, which he presented to Mr. Rosa. CW 6 said that Mr. Rosa had final approval over the budgets that CW 6 presented to him before Mr. Rosa and Defendant Hoffmeister presented the budget to Defendant Sorenson, who then presented the budget to the Board. CW 6 said he believed the Board was presented with budgets indicating the costs of the

items and projects that Mr. Rosa retained from CW 6's original budget request. CW 6 recalled that the 2017 supplemental budget he presented to Mr. Rosa included higher than expected cost requests, including for the data center build-up and an additional $10 million for a network upgrade. CW 6 recalled that Mr. Rosa and Mr. Guardino did not approve all of the costs in that 2017 supplemental budget, and that Mr. Rosa and Defendant Hoffmeister presented what was left to Defendant Sorenson, who in turn presented it to the Board.

161. On August 7, 2018, Macquarie released an analyst report which described the integration process as "seemingly flawless" and "almost too easy." This would prove prophetically true.

162. In September 2017, during the integration process, Marriott was presented with another red flag as to potential deficiencies in its data security. Equifax announced a data breach that affected approximately 147 million people. That data breach subjected Equifax to numerous lawsuits and regulatory actions. For example, there is currently a suit for violations of the federal securities laws in discovery in the Northern District of Georgia.[19] Additionally, the FTC recently announced that Equifax reached a settlement with the FTC, the Consumer Financial Protection Bureau, and 50 U.S. states and territories for violations related to that breach for at least $525 million and up to $700 million.

E. The Breach

1. Marriott's Discovery of the Breach and the Initial Revelation to the Public

163. On September 7, 2018, a technology tool called Guardium discovered the Breach. Guardium triggered an alert that a user ran a query of how many entries were in a particular column of a table in the reservation system database. Accenture, Marriott's third party IT

[19] *In re Equifax Inc. Sec. Litig.*, No. 17-cv-3463 (N.D. Ga.)

contractor tasked with running Starwood's reservation database, alerted Marriott's IT department the following day. On September 10, 2018, Marriott brought in third party investigators to perform a review of their hacked systems.

164. On September 17, 2018, the third party investigators identified a remote access Trojan ("RAT") virus. A RAT is a malware program that includes a back door that allows attackers to access, surveil, and even gain administrative control over a computer. On that day, Marriott's IT department notified Defendant Sorenson. On September 18, 2018, Defendant Sorenson notified Marriott's Board of the Breach. Additionally, in early October 2018, the third party investigators found evidence of other malware in Starwood's database, including Mimikatz which searches a device's memory for usernames and passwords.

165. On October 29, 2018, Marriott contacted the FBI to notify them of the tools used by the hackers, the timelines of the intrusion, and any forensic findings the Company or its third party investigators had made so far. In early November 2018, Marriott learned that the Breach stretched all the way back to at least July 2014. At that time, Marriott implemented "endpoint detection technology on devices across the Starwood network."

166. On November 6, 2018, Marriott filed its 3Q 2018 Form 10-Q without disclosing the fact that it had experienced a serious data breach on a critical customer-serving platform, one which management had previously been informed by information security staff had inadequate access controls. Based on the evidence of the Breach and the known vulnerability, management had every reason to assume that its customers' sensitive personal data had been exposed to attackers. Marriott was silent in its 3Q 2018 Form 10-Q as to the Breach, ***and continued to operate the hacked Starwood guest reservation database***, even going so far as to continue to encourage customers to book reservations with the corrupted reservation database.

167. On November 13, 2018, Marriott's investigators discovered evidence that two compressed encrypted files had been deleted from a device they were examining. On November 19, 2018, Marriott learned that those compressed and encrypted files contained personal information. On that day, Marriott finally began preparations to notify affected guests.

168. On November 25 and 26, 2018, Marriott discovered that in both 2015 and 2016, "the attacker had likely created copies of two other tables, which the attacker later deleted." The file names of those tables corresponded to the files names of the two other tables that had been deleted, but Marriott could not recover those files and did not know if they had been taken.

169. On November 29, 2018, (83 days after the Breach was discovered) Marriott provided notice of the Breach to the four major payment card networks and their credit processing vendors, regulators in over 20 foreign countries and territories, state Attorneys General, the FTC, the SEC, and the three major credit reporting agencies. Marriott also provided an update to the FBI.

170. On November 30, 2018, nearly 3 months after discovering the Breach, Marriott made its first public revelations regarding the Breach.[20] Marriott informed the market that approximately 500 million guest records had been affected by the Breach and that the Company had only just begun notifying guests that their personal information had been compromised. The attackers were able to steal names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.

[20] Notably, the average data breach lasts only 266 days before identification and containment but the data breach at Starwood and then Marriott went undetected for 715 days and was not resolved for at least 733 days after the attackers gained access. Rob Sobers, *Data Breach Response Times: Trends and Tips*, Varonis (Mar. 13, 2019).

171. Marriott completed notification of all U.S.-based guests on December 11, 2018. However, at the time the Company announced the Breach it was not able to determine whether the attackers had also stolen the encryption keys – and to this day, Marriott has still not released whether the attackers had also stolen the encryption keys.

172. The market was shocked by the November 30, 2018, revelation and Marriott's stock price was rocked by the news. In a Form 8-K filed before the market opened, Marriott revealed that there was unauthorized access to the legacy Starwood guest reservation database. The Company disclosed that the personal information of guests who made reservations at Starwood properties on or before September 10, 2018, had been exposed to attack. On this date, the Company's stock price fell $6.81, or 5.5%, to close at $115.03 on extremely heavy volume.

173. On November 30, 2018, Cowen released an analyst report discussing Marriott's revelation of the Breach. In that report, Cowen noted that the incident "***may hamper loyalty enrollment***." The report also noted that it had "cause[d] real brand damage" for Marriott.

174. On November 30, 2018, Taylor Telford and Craig Timberg published an article for the Washington Post on the Breach titled *Marriott discloses massive data breach affecting up to 500 million guests*. In that article, Mr. Telford and Mr. Timberg noted that the "breach of the reservation system for Marriott's Starwood subsidiaries was one of the largest in history . . . and was particularly troubling for the nature of the data that apparently was stolen." The article also quoted Edward Hasbrouck, a travel writer and consumer advocate, who said the Breach involved "'extraordinarily intimate data'" and that the "'travel industry has been grossly negligent compared to many industries when it comes to data privacy and security." Additionally, Paige Boshell, an attorney with Privacy Counsel LLC, noted that "'there were significant opportunities for higher scrutiny.'" Mr. Telford and Mr. Timberg also highlighted Starwood's prior breaches.

175. On November 30, 2018, NBC News posted an article by Erik Oritz titled *Marriott says breach of Starwood guest database compromised info of up to 500 million* to its website. In that article, Mr. Ortiz quoted Jake Williams, the president and founder of cybersecurity firm Rendition Infosec, as saying the revelation was "'very inarticulately worded'" and that he was left "'playing guesswork at what some of these statements mean.'"

176. Also on November 30, 2018, Krebs on Security ("Krebs") published an article titled *Marriott: Data on 500 Million Guests Stolen in 4-Year Breach*. In that article, Krebs described the incident as "a massive data breach exposing the personal and financial information on as many as a half billion customers who made reservations at [] Starwood['s] properties over the past four years." Krebs noted the potential for further revelations regarding the severity of the Breach and cited to the breach of IHG's payment systems in 2017. In the IHG breach, the company initially thought that the point-of-sale systems had been breached at the restaurants or bars of only 12 properties. Approximately three months later, however, IHG revealed the breach actually affected more than 1,000 properties, including the payments systems used at the front desks of some of the properties. Krebs also noted that Marriott's Breach was "just the latest in a long string of intrusions involving credit card data stolen from major hotel chains over the past four years."

177. On November 30, 2018, the New York Times published an article by Nicole Perlroth, Amie Tsang, and Adam Satariano titled *Marriott Hacking Exposes Data of Up to 500 Million Guests*. In that article, the reporters noted that Marriott "asked guests checking in for a treasure trove of personal information." The article also stated that the "intrusion was a reminder that after years of headline-grabbing attacks, the computer networks of big companies are still vulnerable." The reporters also noted that in recent years, according to cybersecurity experts,

"the hospitality industry has become a rich target for nation-state hackers looking to track the travel movements and preferences of heads of states, diplomats, chief executives and other people of interest to espionage agencies." The article also quoted Jake Olcott, a VP at Bitsight, a computer ratings company, who said that finding out about a data breach after a merger closes is "'everybody's worst-case scenario.'" Additionally, the article stated that "***[p]rivacy advocates said there was no excuse for a breach to go unnoticed for four years***." Gus Hosein, the executive director of Privacy International, said a company can claim to take security seriously, ***"but they don't if you can be hacked over a four-year period without noticing."***

178. Also on November 30, 2018, NPR posted an article, written by Avie Schneider, titled *Marriott Says Up To 500 Million Customers' Data Stolen In Breach* to its website. In that article, Schneider noted Marriott's stock fell 5.6% and that the "data breach is one of the largest in history" that included "sensitive data such as passport numbers, mailing addresses and credit card information." The article also quoted Ted Rossman, an analyst with CreditCards.com, who said the Breach is "'one of the most significant data breaches in history given the size . . . and the sensitivity of the personal information that was stolen.'"

179. On November 30, 2018, the LA Times also posted an article, written by Sam Dean, titled *Marriott data breach exposes up to 500 million guests' personal information* to its website. In that article, Dean noted that as a result of the Breach "new laws in Europe could stick the global hotelier with hundreds of millions of dollars in fines." Dean stated that "experts say too many companies continue to have a startlingly lax approach to data security." The article also noted that Marriott's stock fell 5.6%.

180. On December 4, 2018, Forbes posted an article, written by David Volodzko, titled *Marriott Breach Exposes Far More Than Just Data* to its website. The article noted that as a

result of the Breach, Marriott's shares had fallen 5.6%. Additionally, Volodzko noted that Marriott's revelation ***"leaves the question of why [the Company] only now detected a problem that evidently began four years ago."*** The article quoted Andrei Barysevich, a researcher with Recorded Future, a threat intelligence company, who said that ***with all the resources Marriott has, "'they should have been able to isolate hackers back in 2015.'"*** Volodzko noted that "the whole problem began" when Marriott announced the Merger in November 2015 and that "***it's hard to believe Marriott couldn't see [the breach] coming***," particularly because "[h]otels are easy targets, constituting 92% of all point-of-sale intrusions in 2017." Volodzko noted that the prior breaches of Starwood's systems put Marriott on alert that the Company "was clearly taking on considerable risk by acquiring Starwood." Volodzko questioned whether Marriott was "unaware of this danger or was [the Company] using some version of the recall coordinator's formula, putting customers at risk because it assumed the cost of a breach would be less than the cost of better security?" Volodzko quoted John M. Simpson, a project director for privacy and technology at Consumer Watchdog as stating "many companies opt for inadequate data security because it's cheaper than the consequences of a data breach." Volodzko also pointed out that the "ripple effect of a hotel breach goes well beyond customers" due to the interconnectedness of the business entities within a hotel.

181. On December 5, 2018, UBS released an analyst report discussing the Breach. In that analyst report, UBS listed a number of issues the Company would need to address as a result of the Breach, including legal costs, security costs, and potential settlement costs. UBS also noted other issues, such as the Breach taking management's attention away from regular operations, any potential impact on hotel owners, and the impact on enrollment in the Company's loyalty program.

182. On December 14, 2018, Bloomberg posted an article, written by Patrick Clark, titled *Marriott Breach Exposes Weakness in Cyber Defenses for Hotels* to its website. In that article, Clark stated that "[l]ong before Marriott International Inc. disclosed a massive security breach, the hotel industry had earned the dubious reputation as a hospitable place for hackers." In that article, John Burns, the president of Hospitality Technology Consulting, noted that the "longstanding tradition of an innkeeper," to allow customers to sleep safely and securely, has not always extended to the "digital environment."

183. In an article for TechCrunch published on January 4, 2019, Zack Whittaker noted that Marriott had allowed attackers to take "the sort of data that remains highly valuable for spy agencies that can use the information to track down where government officials, diplomats and adversaries have stayed – giving insight into what would normally be clandestine activities."

184. On March 7, 2019, David Shepardson published an article for Reuters discussing Defendant Sorenson's testimony in front of the Senate's Permanent Subcommittee on Investigations. Mr. Shepardson noted that Committee Chairman Portman commented on the point-of-sale breach that Starwood revealed just days after the Merger was announced. Further, the article noted that Senator Carper said that Marriott "acquired a company with 'serious cybersecurity challenges and had actually been attacked before' but chose to initially leave Starwood's security system in place after acquiring it."

185. On March 11, 2019, Kate O'Flaherty published an article for Forbes called *Marriott CEO Reveals New Details About Mega Breach*, in which she noted that ***Marriott took nearly three months to inform the public of the breach.*** Additionally, Ms. O'Flaherty pointed out that Marriott "failed to protect valuable customer information" and that Marriott is "the subject of class action lawsuits that could cost it hugely."

186. On March 22, 2019, Patrick Nohe posted a blog for Hashed Out in which he noted that the identity of the attackers in the Breach could not make Marriott any less culpable for its failure to protect its customers' data. Mr. Nohe identified at least three issues with Marriott's conduct related to the Breach: (1) the Breach lasted for four years; (2) that Marriott failed to discover the Breach during its due diligence; and (3) that it waited months to disclose the Breach.

187. Notably, Senator Elizabeth Warren initiated an investigation into Equifax for their data breach and produced a report of her findings (the "Warren Report"). The Warren Report criticized Equifax for similarly waiting to disclose the breach. After discovering the breach but before telling the public, Equifax held a conference in which it remained silent about the breach. The Warren Report noted that Equifax missed "key opportunities to inform investors of risks" in waiting 40 days to inform the public of suspicious activity in its network and failing to say anything at that conference. The SEC has also stated that "an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident."[21]

2. Marriott's Response to the Breach

188. In response to the Breach, Defendant Sorenson said Marriott was finally shutting down Starwood's corrupted guest reservation database. On December 18, 2018, more than two years after closing the acquisition of Starwood (and 102 days after discovering the Breach), Marriott finally stopped using Starwood's guest reservation database for business operations.

189. Additionally, for the Starwood network Marriott began malware removal, deployment of endpoint protection tools to approximately 70,000 devices, and eventually increased that number to 200,000. Defendant Sorenson claimed the endpoint detections devices

[21] SEC Release Nos. 33-10459; 34-82746, "Statement and Guidance on Public Company Cybersecurity Disclosures"

would "allow real-time discovery of suspicious behavior on both the Starwood and Marriott networks and have next-generation anti-virus features." Consistent with CW 1's testimony, Marriott was only willing to install these security measures after a breach rather than in response to the numerous red flags Marriott was aware of regarding Starwood's systems. Defendant Sorenson also touted Marriott's new-found commitment to "identity access management, which means a broader deployment of two-factor authentication across our systems, as well as network segmentation, which means isolating the most valuable data so that it becomes more difficult for attackers to access the systems and for malware to spread through the environment." Defendant Sorenson did not offer any explanation as to why Marriott had not undertaken any of these measures sooner.

190. As for the guests affected by the Breach, Marriott offered some limited security measures in an attempt to lessen the possibility that the sensitive customer data stolen in the Breach would be used. Marriott set up a website and dedicated call center to address customer concerns regarding the Breach. The Company offered one year of enrollment in WebWatcher.[22]

191. There were security issues with Marriott's remedial measures, however. For example, Marriott used email to notify guests, but the domain name the email was sent from was not Marriott's. Rather, the domain name, "email-marriott.com" is actually registered to a third party firm, CSC. The domain does not load, nor does it have an identifying HTTPS certificate.[23] The only way customers were able to verify the validity of the domain was a note lost in the other information on Marriott's notification site for the Breach. According to cybersecurity

[22] According to Marriott: "WebWatcher monitors internet sites where personal information is shared and generates an alert to the consumer if evidence of the consumer's personal information is found."

[23] HTTPS (Hyper Text Transfer Protocol Secure) appears in the URL when a website is secured by an SSL certificate. The details of the certificate, including the issuing authority and the corporate name of the website owner, can be viewed by clicking on the lock symbol on the browser bar.

experts, the domain was easily spoofable,[24] which put the victims of the Breach at even further risk. Jake Williams, founder of Rendition Infosec, actually registered the domain, "email-marriot.com," with Marriott misspelled, to prevent hackers from using it to try to take further advantage of Marriott's customers. Additionally, Nick Carr of the security firm FireEye registered "email-mariottt.com" for the same reason.

192. Ensuring reliable and unambiguous communication with customers is a fundamental safeguard for any company that relies on eCommerce. The fact that Marriott did not register obvious misspellings of their own domain name and did not have a breach response plan that included communicating with customers in a reliably secure manner indicates that, despite all the red flags and the discovery of an actual breach, Marriott did not have a cybersecurity professional assigned to the systematic prevention and response to a customer data breach.

3. Post-Class Period

193. Following the revelation of the Breach, Marriott continued to inform the market of the steps it was taking to make up for its lax security. These remediation measures show the extent of the gap between Marriott's statements to the public regarding the operation and due diligence surrounding Starwood's guest reservation database.

194. On December 5, 2018, Defendant Oberg admitted that due to the Breach, Marriott "had an ongoing data security program for a while." Additionally, Defendant Oberg stated that as a result of the Breach, the Company had to "step[] up" its investment in the security of the Company's data. Clearly, Marriott had not been doing enough to protect its customers' sensitive personal information, and the due diligence that should have identified the vulnerable systems was inadequate - despite Marriott's representations to the contrary throughout the Class Period.

[24] Domain spoofing, a common form of phishing, occurs when an attacker appears to use a company's domain to impersonate a company or one of its employees.

Defendant Oberg admitted that Marriott "had a plan" but "as a result of [the Breach], we're stepping it up even faster." Defendant Oberg also pointed out that "there's already been dramatic improvement of kind of ways that can quickly, quickly identify that somebody is trying to get into your system." However, Defendant Oberg failed to explain why Marriott failed to utilize any of these advancements in operating and monitoring Starwood's systems.

195. On January 4, 2019, Marriott issued a follow-up press release on the Breach. The Company announced that 383 million guest records were affected by the Breach. Of these 383 million guest records, 5.25 million unencrypted passport numbers were stolen, along with more than 20 million encrypted passport numbers. That number also included 8.6 million encrypted payment cards. The Company also revealed, for the first time, that some of the payment cards may have been unencrypted card numbers, which had been inadvertently entered into the wrong column.

196. On January 4, 2019, Cowen released an analyst report discussing Marriott's follow-up revelations regarding the Breach. In that report, Cowen noted that the Company was reporting the potential that unencrypted payment card numbers were involved for the first time. Additionally, an USA Today article dated January 4, 2019, by Nancy Trejos, acknowledging the announcement that unencrypted payment card numbers may have been involved. Most of the reaction, however, focused on the fact that more than 5 million unencrypted passport numbers were stolen.

197. On March 7, 2019 Defendant Sorenson and the CEO of Equifax, Mark Begor testified before the Senate Permanent Subcommittee on Investigations. Both Defendant Sorenson and Mr. Begor answered questions from Senators regarding the deficiencies in the two companies' data security. During that hearing, several Senators criticized Defendant Sorenson

and Marriott for their deficient due diligence during the Merger and lax security procedures in operating the reservation database. Senator Tom Carper questioned Marriott's data retention policies and stated that he did not "know why [Marriott] would need to have maintained records of millions of guest passport numbers as appears to have occurred in this case." He said that the Breach "raises questions about the degree to which cybersecurity concerns do and should play a role in merger and acquisition decisions." He also noted that "Marriott acquired a company that it knew had serious cybersecurity challenges and had actually been attacked before" and that "[d]espite this, Marriott chose to initially leave Starwood's security system in place after acquiring the company." Senator Carper said the committee was interested in "learn[ing] more about the priority that Marriott executives chose to place on addressing security flaws at Starwood as it worked to integrate its systems into its own." In a Washington Post article titled *Senators slam Equifax, Marriott executives for massive data breaches* published on March 7, 2019, Tony Romm noted that "lawmakers [] faulted Marriott for moving too slowly" to phase out Starwood's systems. Specifically, Senator Rosen was "surprise[d] that Marriott had taken 'no method of auditing the data coming across' in the early days" of the integration.

198. On March 7, 2019, David Shepardson published an article for Reuters discussing Defendant Sorenson's testimony in front of the Senate's Permanent Subcommittee on Investigations. Mr. Shepardson noted that Committee Chairman Portman commented on the point-of-sale breach that Starwood revealed just days after the Merger was announced. Further, the article noted that Senator Carper said that Marriott "acquired a company with 'serious cybersecurity challenges and had actually been attacked before' but chose to initially leave Starwood's system in place after acquiring it."

4. Litigation and Regulatory Action Against Marriott

199. The fallout from the second largest data breach in history has also included the filing of approximately 100 lawsuits against Marriott and Starwood from a variety of plaintiffs, including residents of all fifty states and foreign citizens in American and Canadian court. The lawsuits against Marriott include claims for violations of the data protection laws of all fifty states ("Consumer Track"), as well as derivative claims brought on behalf of Marriott's shareholders and the Company itself (as a nominal defendant), claims from financial institutions regarding their costs stemming from the Breach ("Financial Institution Track"), and claims on behalf of the citizens of Chicago affected by the Breach brought by the City of Chicago (the "Government Track"). Marriott is also facing investigations from "certain committees of the U.S. Senate and House of Representatives," and "regulatory authorities in various other jurisdictions."

200. In connection with the Breach, three amended complaints have already been filed in parallel actions. The plaintiffs in those actions were provided with the Payment Card Industry Forensic Investigation Report ("PFI Report") while drafting their amended complaints.[25] After viewing the PFI Report, plaintiffs in each of the Government Track[26], the Financial Institution Track[27], and the Consumer Track[28] made allegations in their amended complaints regarding Marriott's failure to perform adequate due diligence during the Merger.

---

[25] After a breach, payment card processors are required by the PCI to hire a Payment Card Industry Forensic Investigator ("PFI") to conduct a forensic examination. The company is required to submit a final PFI Report to the PCI.

[26] *Chicago v. Marriott Int'l, Inc.*, No. 19-cv-654, ECF Nos. 294, 296, & 298 (D. Md.) (cited as Government at ¶__)

[27] *Bank of Louisiana v. Marriott Int'l, Inc.*, No. 18-cv-3833, ECF Nos. 306 & 328 (D. Md.) (cited as Financial Institution at ¶__)

[28] *In re Marriott Int'l Inc. Customer Data Sec. Breach Litig.*, No. 19-md-2879, ECF Nos. 346, 351, 352 (D. Md.) (cited as Consumer at ¶__)

201. For example, the Financial Institution Track plaintiffs noted that "[m]any of these [redacted] security deficiencies were the same ones identified by previous security assessments of Starwood's systems and databases." (Financial Institution at ¶ 18). Additionally, the Financial Institution Track's amended complaint, based on its review of the PFI Report, alleged that Marriott committed "numerous violations of the PCI DSS requirements." (Financial Institution at ¶ 59). Further, the Government Track's amended complaint noted that the filing of that action was prompted by a request from the Commissioner for the City of Chicago Department of Business Affairs and Consumer Protection, Rosa Escareno, after she completed her investigation into the Breach. (Government at ¶ 10 n.7). While the Consumer Track filed a document with sweeping redactions, the amended complaint has an entire section titled *An Independent Report Confirms Marriott's Deficient Data Security Practices* which details Marriott's violations of the PCI DSS. (Consumer at ¶¶ 222-38). Though the specific violations were redacted, the Consumer Track notes that "it is highly probable that at least one or more threat actors had already accessed, exfiltrated the files containing encrypted cardholder values, and ascertained how to decrypt the files. (Consumer at ¶ 232). Additionally, the amended complaint for the Consumer Track detailed Marriott's violations of the FTC Act. (Consumer at ¶¶ 254-59).

202. Additionally, as the Company disclosed at the end of Q1 2019, Marriott has spent more than $70 million on remedial measures. Though most of those costs have been reimbursed by insurance thus far, Marriott has noted in its SEC filings that the Breach could make insurance unavailable. Additionally, Marriott is being investigated by the Attorneys General of all fifty states and the District of Columbia, the FTC, and the SEC. Further, on July 9, 2019, the ICO announced its intention to fine Marriott more than $120 million for failure to comply with

GDPR. The ICO's investigation ***"found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems***." The ICO will consider comments from EU residents who were affected by the Breach, and Marriott before making a final ruling on the fine.[29]

F. Marriott Violated Various IT and Security Standards During Its Due Diligence of Starwood's IT Systems, During the Integration Process, and Operation of Starwood's Database

203. Before and during the Class Period, Marriott was required to comply with a number of industry standards. These industry standards required that Marriott keep its customer data safe and secure by using generally accepted reasonable security practices. Despite telling the market that they used "reasonable" efforts to protect customer data, Marriott failed to comply with these standards and reasonably accepted practices in the industry. Marriott's failure to adhere to these industry standards and reasonable practices rendered their Class Period statements about the effectiveness of the due diligence process, and the success of the integration false and misleading when made. Marriott's failure to adhere to these industry standards and reasonable security practices also rendered their risk warnings about the integration and cyber security false and misleading, because they failed to provide the facts about their non-compliance to the market.[30]

1. Due Diligence Standards

204. For Mergers and Acquisition ("M&A"), due diligence is typically driven by executive management and a collection of chosen leaders. Technology is usually a focal point of the due diligence and cybersecurity is a major consideration in technology due diligence,

[29] Separately, the ICO has opened two other investigations into Marriott; one for its online privacy policy, and one into how Marriott handles data subject access requests.

[30] This section was prepared with assistance from an expert in IT cyber security and compliance, including expertise in the requirements for IT due diligence.

particularly where, as here, customer data is one of the primary drivers of the acquisition. For an effective due diligence process, management should clearly lay out the objectives for the merger, identify the assets of the acquisition target that are expected to be preserved and utilized post-acquisition, and form multiple teams of trusted evaluators organized by asset type.

205. It has been recognized for decades by both legal and technology members of M&A teams that technology due diligence should include data privacy and information security review. While the due diligence process is not a prescribed industry standard, the acquiring company is expected to focus on the aspects of the due diligence that are most important, or that pose the most significant risk. In this case, the customer data, and thus the reservation system, were of particular importance to the Company, the Merger and the market. Additionally, Starwood's IT systems were known to be particularly risky, and therefore should have been a subject of intense focus. If Marriott's due diligence team was constrained in its testing for vulnerabilities at Starwood during its due diligence review, it had ample opportunity to iteratively repeat the review in the form of a professionally conducted audit of the Company's reservation database in the intervening two years before the discovery of the Breach.

206. A due diligence review of a target company's information security systems is generally conducted based on an existing due diligence paradigm. For example, in 2014, the internationally peer-reviewed Information Systems Audit and Control (ISACA) Journal published recommendations for management participation in Information Systems due diligence in the form of a *Responsible, Accountable, Consulted and Informed* ("RACI") matrix.[31] A RACI matrix lists activities performed in a process as rows and the organizational participants as columns. The letters in the intersection of a row and a column indicate that the organizational

[31] Bostjan Delak & Marko Bajec, "Conducting IS Due Diligence in a Structured Model Within a Short Period of Time," 4 ISACA J. 1 (2014).

participant in the column heading has an obligation to participate in the activities labeled in the row. The letters in the intersections are "R", "A", "C", or "I" and the letters indicate the role of the individual in the column with respect to the activity in the row. The roles indicated by the letters in the column are:

- "R" - Responsible: the individual performs the activity
- "A" - Accountable: the individual is the authority and decision-maker responsible for the quality of the task performance, the individual is expected to provide oversight and endorse the outcome of the process, or
- "C" - Consulted: the individual contributes knowledge and participates in two-way communication with those responsible and accountable as the activity is planned and executed
- "I" - Informed: the individual receives one-way communication on the details of the activity, typically from those responsible

207. The ISACA due diligence process RACI matrix is detailed in the graphic below. It shows that the CEO is the individual in the organization who is accountable for the information security due diligence process and is accountable for presenting it to the Board. It also shows that the CIO is responsible for conducting the due diligence and is expected to consult the entire executive management team in the process.

Activity		Chief Executive Officer	Chief Financial Officer	Chief Operations Officer	Business Process Owners	Project Management Office	Privacy Officer	Compliance	Human Resources Manager	Audit Manager	Chief Information Security Officer	Chief Information Officer	Head Architect	Head of Development	Head of IT Operations	Database Administrator	LAN/WAN Administrator	Developer	System Administrator	Help Desk Team	Other IT Personnel	IS Due Diligence Team Leader/Manager	IS Due Diligence Team
Make decision for activating IS due diligence.		A	I	R				C	I	C		R										C	
Prepare for IS due diligence.							C	I		C	C	R	R	R	R	R	C	C	C	C	C	A	R
Conduct due diligence.	Interviews with IT											R	C	C	C	C	C	C	C	C	C	A	R
	Interviews with end user	C	C	R	C	C	C	C	C	C	C											A	R
	Visiting IT premises						I			C	C	I		I	R		I	I	I	I	I	A	R
Analyze gathered data.		I		I								I										A	R
Prepare the report.		I		I								I										A	R
Present the report to the board.		A	R	C	I	I	C	I	C	C	C	R	C	C	C	I	I		I			R	I

208. The most authoritative publicly available cybersecurity control assessment guidance is published by the U.S. National Institute of Standards and Technology (NIST), in Special Publication 800-53A ("NIST-SP800-53").[32] NIST-SP800-53 contains dozens of information security control assessment steps that may be expected to be performed by independent technology auditors during technology assessments and audits such as IS Due Diligence reviews.

209. For example, had Marriott engaged professional technology auditors as a part of M&A due diligence, the auditors would have performed technology due diligence following guidance such as that as laid out by NIST-SP800-53. They would have obtained documentation of or themselves documented the flow of customer data within Starwood's systems, including the reservation system. They would have verified that a list of allowed information flows both existed, and that they were authorized by management. Under Marriott's supervision, the auditors also would have examined policies, procedures, and configuration settings for all of the technology devices that were traversed by that data flow. The auditors would also have performed tests to ensure that data flows not on the allowed list did not work, and that there were audit trails of all actual data flows. These tests would allow them to evaluate whether Starwood management enforced approved authorizations for controlling the flow of customer information within its systems and between interconnected systems based on information flow control policies.

210. The auditors would have used the results from the evaluation to: (i) identify the method by which audit records of actual information flows were recorded and preserved, and (ii)

[32] National Institute of Standards and Technology (NIST) Special Publication 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, Dec. 2014.

compare the list of authorized information flows to the audit records to make sure there were no exceptions. They would also have attempted to execute an unauthorized data flow and observed whether or not it resulted in an alert that was investigated using a standard cybersecurity operations procedure.

211. Also at the due diligence stage, and continuing periodically thereafter, Marriott should have conducted vulnerability scans at the network level, the operating system level and at the code level for all the software they were purchasing. These measures are taken not just for security, but are a part of compliance and contractual duties, such as with PCI DSS, as well. In particular, the reservation database should have been given special attention given that it had highly sensitive information and an externally facing interface with third party communication (like Expedia or TripAdvisor to make reservations). During the due diligence process, Marriott should have also prepared and adhered to a schedule to make sure to scan all internet facing applications at a periodic interval corresponding to changes to the system or its environment (in this case, change occurred at least annually). Additionally, Defendants should have examined the actual software and operating systems of the machines and systems they were purchasing in order to make sure there was no unauthorized or unlicensed software, especially no Trojan Horses, malware, or back door access. Moreover, as part of the due diligence review, Marriott should have tested the security of the access control features of the business applications running on the systems. In addition to the focus on critical applications such as the reservations database, a key aspect of any technology due diligence process is the need to make an inventory of the systems, applications, and software. Marriott should have completed that inventory, and after completing the system inventory, Marriott should have examined each system as described above as part of the due diligence process (and thereafter).

212. Further, and most relevant here, Marriott needed to perform due diligence on Starwood's access logs. As a part of adequate IT security, Starwood should have been monitoring access to its systems and correlating each login to an authorized user. While Marriott would not have been expected to manually review these logs and check each login, they should at a minimum have verified that Starwood had a method to correlate each administrative login to an authorized user performing a necessary task, and an automated procedure to detect anomalous access among non-administrative staff, third parties, and customers. Post-acquisition, Marriott should have repeated these access control monitoring procedures to ensure they worked adequately and that log anomalies were investigated. ***Given that the Breach began at least as far back as July 2014, either Marriott knew that Starwood did not have adequate access log correlation procedures or Marriott did not review them and was severely reckless in assuring the market the Company had performed extensive due diligence and maintained adequate data security***.

2. PCI DSS

213. Marriott is also subject to the PCI DSS. Marriott's requirement to comply with PCI DSS stems from the Company's contractual obligations as a credit card payment merchant and processor. PCI DSS has been in force since 2004 and applies to all merchants who accept payment cards and any other organization in the card payment processing lifecycle. Since 2006, the requirements have been set by the PCI Security Standards Council (the "Council"),[33] which consists of American Express, Discover, JCB International, MasterCard and Visa Inc. Each company shares equally in governance and execution of the Council's work.

[33] The Council was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc. They share equally in governance and execution of the Council's work

214. PCI DSS is a highly prescriptive standard that sets forth specific technical safeguards to protect data in processing, storage, and transit. It specifies technology control requirements, testing procedures, and explanatory guidance with which payment processors like Marriott must comply. PCI DSS requires credit card merchants and processors to: (1) build and maintain a secure network; (2) protect cardholder data; (3) maintain a vulnerability management program; (4) implement strong access control measures; (5) regularly monitor and test networks; and (6) maintain an information security policy. These requirements are codified into 12 sections, each with between 2 and 10 subsections that enumerate multiple detailed technical controls. Credit card merchants and processors are further required to hire Qualified Security Assessors (QSAs) to independently verify and validate evidence that all requirements are met.

215. Publicly available information on the Breach indicates clear violation of the PCI DSS standard.[34] Based on publicly accessible information and information provided by former employees/contractors, requirements that Marriott has violated are listed below in the table below. The true extent of Marriott's violations, however, has been enumerated in the PFI Report that Marriott created to comply with its contractual duties. Accordingly, the table below contains only the most obvious of Marriott's PCI DSS violations as a result of the Breach based on publicly available information.

PCI DSS Violations			
#	**Section**	**Subsection**	**Requirement**
1	Install and maintain a firewall configuration to protect	Build firewall and router configurations	1.2 - Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

[34] To ascertain compliance with the requirements, Marriott's Cyberattack was compared to version PCC-DSS Version 3.2, which was the version in effect at the time of the merger. Version 3.2 was released in April 2016, and has been retired since December 31, 2018.

PCI DSS Violations			
#	**Section**	**Subsection**	**Requirement**
2	cardholder data		1.2.1 - Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
3			1.2.3 - Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
4		Prohibit direct public access to system components	1.3 - Prohibit direct public access between the Internet and any system component in the cardholder data environment.
5			1.3.1 - Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
6			1.3.4 - Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
7	Do not use vendor-supplied defaults for system passwords and other security parameters	Develop configuration standards for all system components	2.2.4 - Configure system security parameters to prevent misuse.

PCI DSS Violations			
#	**Section**	**Subsection**	**Requirement**
8	Protect stored cardholder data	Store minimum required cardholder data	3.1 - Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: (i) Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements (ii) Specific retention requirements for cardholder data (iii) Processes for secure deletion of data when no longer needed (iv) A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.
9		Document and implement all key-management processes	3.6.3 - Secure cryptographic key storage.
10	Restrict access to cardholder data by business need to know	Minimize access based on job function	7.1 - Limit access to system components and cardholder data to only those individuals whose job requires such access.
11	Assign a unique ID to each person with computer access	Multi-factor authentication	8.3 - Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.
12			8.3.2 - Incorporate multi-factor authentication for all remote network access (both user and administrator, including third party access for support or maintenance) originating from outside the entity's network.
13	Track and monitor all access to network resources and cardholder data	Review security events	10.6 - Review logs and security events for all system components to identify anomalies or suspicious activity.

PCI DSS Violations			
#	**Section**	**Subsection**	**Requirement**
14	Regularly test security systems and processes	Use intrusion-detection	11.4 - Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

3. FTC Act

216. Additionally, Marriott is required to comply with the FTC Act. Section 5 of FTC Act requires all corporations to refrain from unfair or deceptive acts or practices in or affecting commerce, which includes data security. In its settlement with Wyndham, the FTC essentially laid out a roadmap for compliance with the FTC Act as it relates to data security.[35] In that case, the FTC made clear that lack of security in a hotel company that purports to have "reasonable security" constitutes deceptive and fraudulent practices. The FTC brought charges against Wyndham for three separate data breaches that allowed attackers to steal the payment card information of more than 500,000 customers. The attacks were spread out over a two-year period and Wyndham's customer data was accessed by hackers via a local network at a hotel and also using an administrative account in the Wyndham data center. As a result of that settlement, the FTC required Wyndham to create a comprehensive information security program, and have it audited annually by a qualified, objective third party. That program was required to include:

- a designated employee or employees to coordinate and be held responsible for the program;

[35] *FTC v. Wyndham Worldwide Corp.*, No. 13-cv-1887, ECF No. 283 (D. N.J. Dec. 11, 2015).

- a risk assessment including consideration of (1) employee training and management; (2) information systems, including storage and transmission; (3) company-specific risks; and (4) "prevention, detection, and response to attacks, intrusions, or other systems failure";
- the design and implementation of safeguards to control the risks identified through that assessment;
- regular monitoring and testing of the effectiveness of the key controls, systems, and procedures of the safeguards;
- identifying and retaining capable third parties to safeguard payment card information and including contractually required safeguards in agreements with those third parties; and
- evaluating and adjusting the company's information security program in light of the above-mentioned assessments.

217. In 2015, and relevant to Starwood's Oracle operating system, the FTC issued guidance which stated "[o]utdated software undermines security. The solution is to update it regularly . . . having a reasonable process in place to update and patch third party software is an important step to reducing the risk of a compromise."

To provide guidance for companies that want to make sure their security practices will not be found unreasonable, the FTC has published a guide for business called, "Start with Security." The guide lists ten information security "lessons learned" from enforcement actions and these are listed in the table below. Were the ten practices recommended by the FTC codified as regulation, Marriott would have violated at least eight of 10, as shown in bold below in the table below.

#	FTC Guidance Violations
1	**Factor security into the decision making in every department of your business – personnel, sales, accounting, information technology, etc…**
2	**Control access to data sensibly.**
3	**Require secure passwords and authentication.**

#	FTC Guidance Violations
4	**Store sensitive personal information securely and protect it during transmission.**
5	**Segment your network and monitor who's trying to get in and out.**
6	**Secure remote access to your network.**
7	Apply sound security practices when developing new products.
8	**Make sure your service providers implement reasonable security measures.**
9	**Put procedures in place to keep your security current and address vulnerabilities that may arise.**
10	Secure paper, physical media, and devices.

218. The FTC has also issued a memo that endorses the NIST-CSF as a good source of fundamental security practices because that cybersecurity industry standard aligns with FTC objectives.[36] The FTC has publicly stated that NIST-CSF guidance is aligned with its own standards for enforcing compliance with the FTC Act, and as such the NIST-CSF can be used as a proxy for an actual FTC publication on the topic. The FTC memo on NIST-CSF states:

> The types of things the Framework calls for organizations to evaluate are the types of things the FTC has been evaluating for years in its Section 5 enforcement to determine whether a company's data security and its processes are reasonable. By identifying different risk management practices and defining different levels of implementation, the NIST Framework takes a similar approach to the FTC's long-standing Section 5 enforcement.[37]

219. Although NIST-CSF is not an implementation checklist, it does list five basic cybersecurity functions expected to be in place at organizations at various levels of cybersecurity program sophistication, and suggests that businesses rate their cybersecurity risk management capability using four "tiers": (1) Partial; (2) Risk Informed; (3) Repeatable; and (4) Adaptive.

[36] The NIST operates under the supervision of the Department of Commerce. On its website, the NIST says it "strives to be a leader in best privacy practices and privacy policy."

[37] Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FTC Business Blog (Aug. 31, 2016)

An explanation of these four tiers is attached hereto as Exhibit A.[38] NIST-CSF encourages organizations to manage cybersecurity risk at Tier 2 ("Risk Informed") or greater, depending on their own risk profile. In consultation with a cybersecurity expert and after reviewing publicly available information, Lead Plaintiff has determined that the risk management capability within Marriott's cybersecurity program would be classified in the "Partial" tier.

The NIST-CSF has describes a type of closed-loop cybersecurity risk management cycle, in which the output of risk management activities feeds into the other activities, continuously combining these five basic functions: (1) Identify; (2) Protect; (3) Detect; (4) Respond; and (5) Recover. The five functions are then decomposed into categories of cybersecurity outcomes that generally correspond to aspects of enterprise cybersecurity programs. These categories are further divided into specific measurable outcomes of technical and/or management activities. These subcategories provide an exemplar set of results that help shape enterprise efforts to produce the outcomes. The table below details NIST-CSF subcategories that Marriott failed to achieve. Note that this list, like the PCI DSS violations listed in the table in ¶ 215 is based on publicly available information and information obtained from former employees/contractors. It would likely be expanded if more details on Marriott's security program were available.

NIST-CSF Guidance Violations			
#	**Function**	**Category**	**Subcategory**
1	Identify	Governance	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
2		Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented
3	Protect	Identity	PR.AC-3: Remote access is managed

[38] *See* attached hereto as Exhibit A.

NIST-CSF Guidance Violations			
#	**Function**	**Category**	**Subcategory**
4		Management, Authentication and Access Control	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
5			PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
6		Data Security	PR.DS-1: Data-at-rest is protected
7			PR.DS-5: Protections against data leaks are implemented
8		Protective Technology	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
9	Detect	Anomalies and Events	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
10		Security Continuous Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events
11			DE.CM-4: Malicious code is detected
12			DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
13			DE.CM-8: Vulnerability scans are performed
14		Detection Processes	DE.DP-2: Detection activities comply with all applicable requirements
15			DE.DP-5: Detection processes are continuously improved
16	Respond	Analysis	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
17		Mitigation	RS.MI-1: Incidents are contained
18			RS.MI-2: Incidents are mitigated

4. GDPR

220. Marriott was also subject to the EU's General Data Protection Regulation (GDPR). GDPR became effective May 2018 and regulates the storage, transmission and

processing of data that is personal to natural persons residing in the EU, regardless of the country in which the business is incorporated and/or operates. For the purposes of GDPR compliance, Marriott is considered both a "data processor" and a "data controller."[39] GDPR fines can reach a maximum of 4% of a company's annual global revenue. Given Marriott's global operations, billions of dollars in annual revenues, and that it caters to European travelers in the United States and globally, the Company had a particular interest in complying with GDPR.

221. GDPR defines the data controller as the party responsible for the protecting personal data and respecting the rights of the data subject, while the processor is any entity that handles personal data while servicing the controller. GDPR Section 4 Articles 24 through 39 define the obligations of data controllers and processors, which include requirements with respect to: (1) data protection by design and by default; (2) records of processing activities; (3) security of processing; (4) cooperation and consultation with the supervisory authority; (5) notification of a personal data breach to both the supervisory authority and the data subject; (6) data protection impact Assessment; and (7) the designation, position, and tasks of a data protection officer. The requirements cross reference each other and also other GDPR Articles that are part of the broader regulation and impact data processes and controller, though may not speak specifically to technology controls. For example, technology controls are covered under more general obligations for Certification and Compliance. Based on public information, the table below details GDPR requirements with which Marriott failed to comply with. Again, this is likely not the full list of Marriott's GDPR violations.

[39] A data controller is defined as "the party that, alone or jointly with others, determines the purposes and means of the processing of personal data." A data processor is the party that actually processes that personal data for the company. Marriott is both a data controller and a data processor for the purposes of GDPR compliance.

GDPR Requirements Violated			
#	**Section**	**Subsection**	**Requirement**
1	General obligations	Responsibility of the controller	24: Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2		Data protection by design and by default	25-1: Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
3			25-2: The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

GDPR Requirements Violated			
#	**Section**	**Subsection**	**Requirement**
4	Security of personal data	Security of processing	32-1: The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
5			32-4: The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.
6	Data protection impact assessment and prior consultation	Data protection impact assessment	35-1: Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risk

GDPR Requirements Violated			
#	**Section**	**Subsection**	**Requirement**
7			35-3: A data protection impact assessment shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.
8			35-7-d: Data protection impact assessment shall contain the measures envisaged to address the risks to data subjects, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
9			35-11: Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

222. As discussed herein, Marriott's violations of GDPR, and potentially other regulations, have manifested in the ICO issuing a notice of its intention to fine Marriott more than $120 million, and a determination that Marriott failed to perform adequate due diligence during the Merger.

5. Privacy Shield and Safe Harbor Principles

223. Marriott informed the public that the Company voluntarily complied with additional standards governing the security of customer data in the EU. Specifically, Marriott

informed the public through starwoodhotels.com that the Company's data security practices were in compliance with the U.S.-EU Safe Harbor Framework ("Safe Harbor Framework"). Additionally, Marriott informed the public through Marriott.com that the Company certified to following the data security requirement laid out in the EU-U.S. Privacy Framework and the Swiss-U.S. Privacy Shield Framework (collectively the "Privacy Shield Frameworks").

224. The U.S.-EU Safe Harbor Framework ("Safe Harbor Framework") was in effect until 2015 and was designed to assist U.S. companies that process personal data collected in the EU in complying with European privacy regulations. The Safe Harbor Framework has seven requirements companies must adhere to in order to attest compliance: (1) notice; (2) choice; (3) onward transfer; (4) security; (5) data integrity; (6) access; and (7) enforcement. First, companies must provide individuals with details on the collection of their data, what it will be used for, and how to get in touch with the company regarding the data. Second, companies must provide individuals with the opportunity to choose how the company uses the individual's data. Third, parties are only able to transfer data to third parties if they've complied with the first two requirements of the Safe Harbor Framework. Fourth, companies "creating, maintaining, using or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction." Fifth, companies can only use personal data for the purpose for which it was collected. Sixth, companies must provide individuals with access to the personal data they have collected on the individual. Seventh, and finally, companies must have mechanisms in place to enforce the preceding requirements, and remedy problems that arise in the context of adhering to the Safe Harbor Framework.

225. The EU-U.S. Privacy Shield Framework became effective in 2016, and the Swiss-U.S. Privacy Shield Framework became effective 2017. The Privacy Shield Frameworks were designed to provide American and European countries with a mechanism to comply with European data privacy requirements when transmitting customer data from Europe to the U.S. The Privacy Shield Frameworks have similar requirements to the Safe Harbor Framework: (1) notice; (2) choice; (3) accountability for onward transfer; (4) security; (5) data integrity and purpose limitation; (6) access; and (7) recourse enforcement, and liability. First, companies must provide adequate notice to individuals regarding the collection, use, and protection of customer data. Second, companies must provide individuals a choice in how the company uses their data. Third, companies must comply with the first two requirements if they are going to transfer the individual's data. Fourth, companies "must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data." Fifth, companies can only process data for the purpose for which it was collected. Sixth, the company must provide individuals with access to their data. Seventh, and finally, companies must have mechanisms in place to address and remedy any issues. Given the observations of the CWs, Marriott knew of issues with the security of customer data and did not address or remedy them, and therefore did not comply with the Privacy Shield Frameworks or the Safe Harbor Framework.

6. COSO Framework

226. Additionally, Marriott, as a publicly traded company, had obligations to maintain safe and secure internal systems so that its sensitive financial and customer data is protected, and so that investors have accurate information regarding the Company. In its 2018 Form 10-K, Marriott stated that the Company used the Internal Control - Integrated Framework issued by the

Committee of Sponsoring Organizations of the Treadway Commission[40] (2013 Framework) (the "COSO Framework") to evaluate the effectiveness of the Company's internal controls. Having effective internal controls requires the Company to safeguard the Company's assets, which in Marriott's case includes the personal data in its guest reservation database. The COSO Framework, with which Marriott has acknowledged it needs to comply, provides rigorous internal control standards for cybersecurity and other operational risks.

227. COSO defines internal control and associated categories of objectives in the areas of operations, reporting, and compliance. In the COSO Framework, internal control is composed of: (1) control environment; (2) risk assessment; (3) control activities; (4) information and communication; and (5) monitoring activities. Each component is elucidated with distinct principles that are clarified with points of focus and evaluation criteria. COSO acknowledges that controls embedded in one component may affect the internal control embedded in another at the entity, division, organizational unit, or function level, so COSO contains a graphic to communicate that it is not possible for components to be managed separately, only holistically. The figure below illustrates the interconnectivity of a company's internal control environment.

[40] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control - Integrated Framework: Executive Summary, Framework and Appendices, and Illustrative Tools for Assessing Effectiveness of a System of Internal Control (3 volume set), First issued in 1992 and most recently updated in May 2013. Note: COSO Members include: American Accounting Association, American Institute of Certified Public Accountants, Financial Executive Institute, Institute of Internal Auditors, Institute of Management Accountants.

The COSO Cube

228. The operations category of the COSO Framework includes the requirement to safeguard assets, *i.e.*, to protect and preserve the company's assets. In Marriott's case, that includes the Company's vast repository of sensitive personal information, and Marriott was required to protect the data it purchased from Starwood beginning ***immediately*** upon the close of the Merger. A foundational requirement of the COSO Framework is that senior management must specify suitable business objectives so that risks to the achievement of enterprise operations, reporting, and compliance objectives, such as safeguarding assets, can be identified and assessed. The COSO framework stipulates that such business objectives should be articulated using attributes that are specific, measurable or observable, attainable, relevant, and time-bound. Additionally, the due diligence process required by the SEC prior to a decision to merge includes immediate planning for control over all acquired operations on day 1 of the lifecycle of the merged entity. Marriott's two-year plan for integrating the systems did nothing to absolve Marriott of liability for the Breach in the guest reservation database at the close of the Merger.

229. Similar to the other standards, Marriott committed numerous violations of the COSO Framework detailed in the table below.

COSO Principles Violated by Marriott		
#	**Component**	**Principle**
1	Control Environment	1. The organization demonstrates a commitment to integrity and ethical values.
2		5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
3	Risk Assessment	9. The organization identifies and assesses changes that could significantly impact the system of internal controls.
4	Control Activities	10. The organization selects and develops control activities over technology to support the achievement of objectives.
5	Information and Communication	14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
6	Monitoring	16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

230. The COSO Framework requirements are process and governance oriented, rather than a prescription for exactly which controls need to be implemented. However, COSO has issued supplemental guidance specific to technology controls. The guidance advises that risk evaluation is aided by comparison of enterprise control activities to technology standards and frameworks that are aligned with the management of cyber risks. The recommended standards for comparison are detailed in table below.

COSO Compliant Technology Standards		
Standard	**Publisher**	**Scope**
ISACA COBIT[41]	The Information Systems Audit and Control Association (ISACA)	Originally Control Objectives for Information Technology, now a set of processes that bridge the gap between technical control issues and business risks
ISO 27000 Series[42]	The International Organization for Standardization (ISO)	A progressively more detailed set of documents that set standards for information security governance process and control implementation.
NIST CSF[43]	National Institute of Standards and Technology of the U.S. Department of Commerce (NIST)	A Framework for Improving Critical Infrastructure Cybersecurity that reduces cybersecurity to five critical functions and maps multiple existing standards, guidelines, and practices to those functions.

231. All of these technology standards are widely used by large global corporations like Marriott. Considered from the perspective on industry standards, COBIT is the least prescriptive of the three recommended in the COSO document. Like COSO, it is principle-based and relies on management to use sound judgement to evaluate and address risk. Yet even by the COBIT standard, Marriott failed to adequately assess the effectiveness of its internal controls in operating the reservation system and database for two years while it contained a breach. There are five COBIT Principles and these are focused on consistency in technology process delivery: (1) meeting stakeholder needs; (2) covering the enterprise end-to-end; (3) applying a single, integrated framework; (4) enabling a holistic approach; and (5) separating governance from

[41] ISACA (2012). COBIT5, A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL, Information Systems Audit and Control Association, IT Governance Institute.

[42] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27000 family - Information security management systems.

[43] National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Department of Commerce, 2018.

management. Additionally, COBIT identifies a specific business goal for "IT compliance and support for business compliance with external laws and regulations." Primary technology processes and corresponding example technology process goals related to that business goal are listed in the table above in ¶ 232. Within COBIT, each IT process is defined not only by its purpose, goals, and key management practices, but also by corresponding management monitoring metrics. All of the processes in the table in ¶ 232 are associated with metrics that include "coverage of compliance assessments." The fact that Marriott has failed so many industry standard assessments indicates that either these metrics did not exist, or that they were not acted upon.

232. Marriott's failures with respect to the COBIT standard are listed below in the table below. As in the case of PCI DSS, this is likely not a complete list.

COBIT STANDARDS VIOLATED			
#	**Process Domain**	**Process Identifier**	**Example IT Process Goal**
1	Align, Plan and Organize	1 - Manage the IT Management Framework	All aspects of the IT strategy are aligned with the enterprise strategy.
2		12 - Manage Risk	A current and complete risk profile exists.
3		13 - Manage Security	Information security solutions are implemented and operated consistently throughout the enterprise.
4	Build, Acquire and Implement	10 - Manage Configuration	Configuration repository is accurate, complete and up to date.
5	Deliver, Service and Support	6 - Manage Security Services	Impact assessments reveal the effect of the change on all affected components.
6	Monitor, Evaluate and Assess	2 - Monitor, Evaluate and Assess the System of Internal Control	Independent assurance that the system of internal control is operational and effective is provided.
7		3 - Monitor, Evaluate and Assess	External compliance requirements are adequately addressed.

COBIT STANDARDS VIOLATED			
#	**Process Domain**	**Process Identifier**	**Example IT Process Goal**
		Compliance with External Requirements	

233. Through its due diligence during the Merger and its operation of the legacy Starwood guest reservation database, Marriott violated industry standards, PCI DSS, the FTC Act, GDPR, the Safe Harbor Framework, the Privacy Shield Frameworks, and COSO. Even a cursory review of the legacy Starwood guest reservation database would have revealed a lack of compliance with these standards. Defendants knew of these violations and repeatedly, and misleadingly, touted Marriott's due diligence and security standards, or Defendants were severely reckless in making statements to the market regarding Marriott's due diligence and security standards without a reasonable basis for doing so. Additionally, these standards require the company to give notice to consumers, which Marriott delayed, as well as U.S. states, federal entities, and European government agencies.

VII. DEFENDANTS' MATERIALLY FALSE AND MISLEADING STATEMENTS AND OMISSIONS DURING THE CLASS PERIOD[44]

A. November 16, 2015 – Prospectus Containing a Letter to Marriott Associates Regarding the Merger

234. The Class Period begins on November 16, 2015, the day the Merger was announced. On November 16, 2015, after the market closed, Marriott filed a Prospectus pursuant to SEC Rule 425 containing a letter from Defendant Sorenson to Marriott associates discussing the Merger and what Marriott's associates should expect. In that letter, Defendant Sorenson stated:

[44] The statements that are ***bolded and italicized*** in this section are statements alleged to be false or misleading.

> This union will also generate tremendous growth: growing value for shareholders, growing choices and benefits for consumers, growing economic advantages for our owners and franchisees, and growing opportunities for associates.
>
> ***This integration will require a significant amount of work, but while the scale is much larger, we have successfully completed integrations before. We have always emerged stronger, and better positioned, to compete in a rapidly changing marketplace.***

235. Also in that letter to Marriott associates, Defendant Sorenson stated: "***The team will guide the Starwood integration and ensure that it succeeds with minimal disruption to our business.***"

236. The Prospectus also contained a letter from Defendant Sorenson to Starwood associates. In that letter, Defendant Sorenson stated:

> Delighting our guests is the priority, ***and we don't anticipate the integration having an impact at the hotel level worldwide.*** There will be some support areas where we overlap and we'll address those in time as we look to more efficiently run our combined organization.

237. The statements concerning the state of the Marriott and Starwood integration were false and misleading when made because they portrayed the integration in a positive light, conveying that the integration would have a minimal impact on Marriott and that Marriott would employ its experience to ensure that the integration would be successful. However, throughout the integration, the legacy Starwood guest reservation database was compromised by the Breach. At the time Defendants made these statements, Starwood's IT systems were severely vulnerable, using an outdated Oracle application portal that could not be updated or patched. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Marriott failed to share this important information with the market. In addition to failing to discover the Breach (despite seeing how vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that should have caused Marriott to discover the Breach

(or at least safeguard Starwood's vulnerable client data before purchasing) including, but not limited to: (1) Starwood's known cybersecurity issues; (2) significant (and public) intrusions into the systems and databases of Marriott's competitors by hackers to gain access to customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen. Moreover, as confirmed by former employees of Marriott, Defendants failed to spend the money or resources needed to ensure that the transformative Starwood integration was actually being carried out adequately, which included ensuring Starwood's IT systems were safe and kept customer data secure.

B. January 27, 2016 – Amendment to the Registration Statement

238. On January 27, 2016, after the market closed, Marriott filed Amendment No. 1 to Form S-4 Registration Statement ("Amendment No. 1") related to the Merger. Amendment No. 1 was signed by Defendant Sorenson. In recommending the transaction to Starwood's shareholders, Marriott's Registration Statement listed a number of factors in favor of stockholders accepting the Merger Agreement, including "***both Marriott's and Starwood's strong track records in merger integration***."

239. Also in Amendment No. 1, when listing the strategic and financial benefits of the Merger, Marriott stated:

> ***All 11 of Marriott's current directors will continue to serve on Marriott's Board with the expected addition of three members of Starwood's current board, ensuring continuity of Marriott's Board and the addition of directors with a deep knowledge of Starwood, enhancing the Marriott Board's understanding of the integration process.***
>
> ****
>
> ***Given Marriott's Board's knowledge of Marriott's business, operations, financial condition, earnings and prospects and Marriott's Board's knowledge of Starwood's business, operations, financial condition, earnings and prospects, taking***

> ***into account Starwood's publicly filed information and the results of Marriott's due diligence review of Starwood, the prospects for the combined company are favorable.***

240. These statements were false and misleading when made because they gave the market a false sense that through the due diligence process and continuity of having Starwood board members join Marriott's Board, Marriott would successfully integrate Starwood to the benefit of Marriott and its shareholders. In particular, Marriott touted the "***strong track record***," "***deep knowledge of Starwood***" that these former Starwood board members had, and told the market that based on the due diligence completed to date, "***the prospects for the combined company are favorable***." However, at this time, the Starwood's guest reservation database was compromised by the Breach, and its systems (and valuable customer data) were vulnerable to attack. Specifically, at the time they made these statements, Starwood's IT systems were severely vulnerable, using an outdated Oracle application portal that could not be updated or patched. The Company's due diligence process would have revealed these glaring and obvious deficiencies, yet Marriott failed to share this important information with the market. In addition to failing to discover the Breach (despite seeing how vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that should have caused Marriott to discover the Breach (or at least safeguard Starwood's vulnerable client data before purchasing) including, but not limited to: (1) Starwood's known cybersecurity issues, including a point-of-sale breach announced just five days after the Merger Agreement was signed; (2) significant (and public) intrusions into the systems and databases of Marriott's competitors by hackers to gain access to customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen. Moreover, as confirmed by former employees of Marriott, Defendants failed to spend the money or resources needed to ensure that

the transformative Starwood integration was going to be carried out adequately, which included ensuring Starwood's IT systems were safe and kept customer data secure.

C. February 16, 2016 – Second Amendment to the Registration Statement

241. On February 16, 2016, after the market closed, Marriott filed Amendment No. 2 to Form S-4 Registration Statement ("Amendment No. 2") related to the Merger. The Amended Registration Statement became effective on February 17, 2016, and was signed by Defendant Sorenson.

242. The amendment repeated the false statements about "***both Marriott's and Starwood's strong track records in merger integration***" and that:

> ***All 11 of Marriott's current directors will continue to serve on Marriott's Board with the expected addition of three members of Starwood's current board, ensuring continuity of Marriott's Board and the addition of directors with a deep knowledge of Starwood, enhancing the Marriott Board's understanding of the integration process.***
>
> ****
>
> ***Given Marriott's Board's knowledge of Marriott's business, operations, financial condition, earnings and prospects and Marriott's Board's knowledge of Starwood's business, operations, financial condition, earnings and prospects, taking into account Starwood's publicly filed information and the results of Marriott's due diligence review of Starwood, the prospects for the combined company are favorable.***

243. These statements were false and misleading when made for the same reasons stated in ¶ 242.

D. February 17, 2016 – Prospectus

244. On February 17, 2016, after the market closed, Marriott filed a prospectus pursuant to SEC Rule 424(b)(3) related to the Merger. The prospectus was signed by Defendant

Sorenson and repeated the false statement made about "***both Marriott's and Starwood's strong track records in merger integration***" and that:

> ***All 11 of Marriott's current directors will continue to serve on Marriott's Board with the expected addition of three members of Starwood's current board, ensuring continuity of Marriott's Board and the addition of directors with a deep knowledge of Starwood, enhancing the Marriott Board's understanding of the integration process.***
>
> ****
>
> ***Given Marriott's Board's knowledge of Marriott's business, operations, financial condition, earnings and prospects and Marriott's Board's knowledge of Starwood's business, operations, financial condition, earnings and prospects, taking into account Starwood's publicly filed information and the results of Marriott's due diligence review of Starwood, the prospects for the combined company are favorable.***

245. These statements were false and misleading when made for the same reasons stated in ¶ 242.

E. February 18, 2016 – Q4 2015 Earnings Call

246. On February 18, 2016, at 10:00 am EST, Marriott held a conference call to discuss Q4 2015 earnings, the Merger, and other topics. On that call, an analyst asked Defendant Sorenson about avoiding pitfalls in an acquisition and Defendant Sorenson stated:

> Analyst
>
> So, if you guys could talk about the challenges that you face integrating the two companies and their systems. We are getting several questions about, going back to the Ryman acquisition, how -- I guess the question really is, what are you doing to be as thorough as you can so that you avoid some of the pitfalls?
>
> Defendant Sorenson
>
> Yes, it is a good question. I think we are hopefully learning from the experiences we have had in the past few years. You can, to some extent, look at the Gaylord acquisition and the Protea and

> Delta acquisitions as warm-up acts for this, I suppose, and hopefully we're getting better at it.
>
> Now at the same time, obviously, Starwood is a much bigger deal than any of those were, which presents some positive differences and then some greater challenges. I think on the positive side Starwood is hopefully less distracted by the process of the sale of the company, and you have got a big, talented group of folks over there running 350,000 rooms or so. But I know the Starwood team, with our encouragement, is very much focused on continuing to drive sales and to drive the development engine, and we have taken steps to try and put our arms around those teams of folks so that they are as little distracted by this as possible.
>
> I think some of the other deals we did early, it was that sales engine which looked like it got distracted during a sales process and to some extent between the negotiator -- the signing of a deal and the closing of a deal.
>
> ***And we are doing everything we can to plan for integration of systems and integration of business units between now and when we close so that we can implement those as quickly as possible. And we're optimistic at this point that this will go well.***

247. The statements concerning the state of the Marriott and Starwood integration were false and misleading when made because they portrayed the integration in a positive light, conveying that the integration would have a minimal impact on Marriott and that Marriott would employ its experience to ensure that the integration would be successful. However, throughout the integration Starwood's guest reservation database was compromised by the Breach. At the time Defendants made these statements, Starwood's IT systems were severely vulnerable, using an outdated Oracle application portal that could not be updated or patched. An adequate merger due diligence process would have easily revealed these glaring and obvious deficiencies, yet Marriott failed to share this important information with the market. In addition to failing to discover the Breach (despite seeing how vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that should have caused Marriott to discover the Breach (or at least safeguard Starwood's vulnerable client data before purchasing)

including, but not limited to: (1) Starwood's known cybersecurity issues, including a point-of-sale breach announced just five days after the Merger Agreement was signed; (2) significant (and public) intrusions into the systems and databases of Marriott's competitors by hackers to gain access to customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen. Moreover, as confirmed by former employees of Marriott, Defendants failed to spend the money or resources needed to ensure that the transformative Starwood integration was actually being carried out adequately, which included ensuring Starwood's IT systems were safe and kept customer data secure.

F. February 18, 2016 – 2015 Form 10-K

248. On February 18, 2016, at around noon, Marriott filed the Company's Form 10-K for year ending 2015 ("2015 Form 10-K"). The 2015 Form 10-K was signed by Defendants Sorenson, Oberg, and Val Bauduin, and made representations regarding the security of customer data, the Company's operations, and the Merger.

249. In the 2015 Form 10-K, in regard to the security of customer data, Marriott stated:

> Keeping pace with developments in technology is important for our operations and our competitive position. Furthermore, ***the integrity and protection of customer, employee, and company data is critical to us*** as we use such data for business decisions and to maintain operational efficiency.

250. This statement was false and misleading when made because, while touting how important data security was to Marriott on the one hand, on the other hand, Marriott was failing to perform sufficient due diligence to ensure that customer data purchased from Starwood was protected. At this time, Starwood's guest reservation database was compromised by the Breach. Indeed, at the time they made these statements, Starwood's IT systems were severely vulnerable, using an outdated Oracle application portal that could not be updated or patched. The Company's merger due diligence process would have easily revealed these glaring and obvious

deficiencies, yet Marriott failed to share this important information with the market. In additional to failing to discover the Breach (despite seeing how vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that should have caused Marriott to discover the breach (or at least safeguard Starwood's vulnerable client data before purchasing) including, but not limited to: (1) Starwood's known cybersecurity issues, including a point-of-sale breach announced just five days after the Merger Agreement was signed; (2) significant (and public) intrusions into the systems and databases of Marriott's competitors by hackers to gain access to customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen. Moreover, as confirmed by former employees of Marriott, Defendants failed to spend the money or resources needed to ensure that the transformative Starwood integration was actually being carried out adequately, which included ensuring Starwood's IT systems were safe and kept customer data secure.

251. Also in the 2015 Form 10-K, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> The combined company may not be able to integrate successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. ***We entered into the Merger Agreement with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner.***
>
> ***The integration process could also take longer than we anticipate and could result in the loss of valuable employees, the disruption of each company's ongoing businesses, processes and systems or inconsistencies in standards, controls, procedures, practices, policies and compensation arrangements, any of which could adversely affect the combined company's ability to achieve the benefits we anticipate. The combined company's resulting portfolio of approximately 30 brands could be challenging for us to maintain and grow, and the harmonization of our different***

> ***reservations and other systems and business practices could be more difficult, disruptive, and time consuming than we anticipate. The combined company's results of operations could also be adversely affected by any issues attributable to either company's operations that arise or are based on events or actions that occur before the Starwood Combination closes.*** The combined company may also have difficulty addressing possible differences in corporate cultures and management philosophies. ***The integration process is subject to a number of uncertainties, and we cannot assure you that the benefits we anticipate will be realized at all or as quickly as we expect.*** If we don't achieve those benefits, our costs could increase, our expected net income could decrease, and the combined company's future business, financial condition, operating results and prospects could suffer.

252. These statements were false and misleading when made because while warning of potential risks related to integrating the business, Marriott failed to disclose critical facts relevant to these risks. In particular, at the time these statements were made, Starwood's IT systems were severely vulnerable, using an outdated portal and software that could not be updated or patched. An adequate due diligence process would have easily revealed these glaring and obvious problems with Starwood's IT department and data security and revealed that there was a dangerous inconsistency in standards and controls (not just a mere risk), yet Marriott failed to share this important information with the market. In addition to failing to discover the Breach (despite seeing how vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that should have caused Marriott to discover the Breach (or at least safeguard Starwood's vulnerable client data before purchasing) including, but not limited to: (1) Starwood's known cybersecurity issues, including a point-of-sale breach announced just five days after the Merger Agreement was signed; (2) significant (and public) intrusions into the systems and databases of Marriott's competitors by hackers to gain access to customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen. Moreover, as confirmed by former employees of Marriott, Defendants failed to spend the

money or resources needed to ensure that the transformative Starwood integration was actually being carried out adequately, which included ensuring Starwood's IT systems were safe and kept customer data secure.

253. Also in the 2015 Form 10-K, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Marriott Rewards and The Ritz-Carlton Rewards programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> ***
>
> *We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data.* Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***
>
> ***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our***

systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.

***

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches.

***

Any disruption in the functioning of our reservation system, such as in connection with the Starwood Combination, could adversely affect our performance and results. We manage a global reservation system that communicates reservations to our branded hotels that individuals make directly with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel web sites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of

> ***our global reservation system could increase in connection with the system integration that we anticipate undertaking following consummation of the Starwood Combination. Disruptions in or changes to our reservation system could result in a disruption to our business and the loss of important data.***

254. These statements were false and misleading when made because while warning of potential risks related to cybersecurity, Marriott failed to disclose critical facts relevant to these risks. In particular, at the time these statements were made, Starwood's IT systems were severely vulnerable, using an outdated Oracle application portal that could not be updated or patched. An adequate due diligence process would have easily revealed these obvious and glaring problems with Starwood's IT department and data security, including that Starwood was not PCI compliant and did not comply with other applicable rules and regulations that Marriott was subject to, yet Marriott failed to share this important information with the market. In addition to failing to discover the Breach (despite seeing how vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that should have caused Marriott to discover the Breach (or at least safeguard Starwood's vulnerable client data before purchasing) including, but not limited to: (1) Starwood's known cybersecurity issues, including a point-of-sale breach announced just five days after the Merger Agreement was signed; (2) significant (and public) intrusions into the systems and databases of Marriott's competitors by hackers to gain access to customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen. Moreover, as confirmed by former employees of Marriott, Defendants failed to spend the money or resources needed to ensure that the transformative Starwood integration was actually being carried out adequately, which included ensuring Starwood's IT systems were safe and kept customer data secure.

G. March 21, 2016 – Conference Call to Discuss Amended Merger Agreement

255. On March 21, 2016, at noon EST, Marriott held a conference call to discuss the Amended Merger Agreement. On that call, Defendant Oberg stated:

> ***After we've had extensive due diligence and spending a lot of time with the Starwood team and joint integration planning,*** we increased our targeted annual G&A cost synergies to $250 million, up from $200 million. And excluding any benefit from even more incremental cost savings beyond the $250 million and additional revenue synergies which we're confident we will provide, we expect adjusted EPS to be roughly neutral in 2017 and 2018.

256. Later on in that conference call, in discussing Marriott's due diligence, Defendant Sorenson stated:

> ***In the further diligence we have completed in last five months, we have become even more convinced of the tremendous opportunity presented by this merger. That confidence is reflected in our higher offer. We now believe there are more cost synergies than we estimated in November.***

257. Later on in that conference call, in discussing the potential cost synergies from the Merger, Defendant Sorenson stated:

> We've talk a little bit about cost synergies. This is now on page 10 for those of you who are following along. ***We have been working intensely since we announced this deal in November to prepare for integration and of course, to understand each other's organizations and structures and start to think about how to meld those into one organization.***

258. These statements were false and misleading when made because they gave the market a false sense that Marriott was performing adequate due diligence on the $13 billion dollar Merger, when it was not. At the time they made these statements, Starwood's IT systems were severely vulnerable, using an outdated Oracle application portal that could not be updated or patched. An adequate due diligence process would have easily revealed these glaring and obvious deficiencies,. In addition to failing to discover the Breach (despite seeing how

vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that should have caused Marriott to discover the Breach (or at least safeguard Starwood's vulnerable client data before purchasing) including, but not limited to: (1) Starwood's known cybersecurity issues; (2) significant (and public) intrusions into the databases of Marriott's competitors by hackers to gain access to customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen.

H. March 21, 2016 – Defendant Sorenson's LinkedIn Post

259. On March 21, 2016, Defendant Sorenson posted a statement to LinkedIn:

> Since we announced the merger in November 2015, our integration teams have met on average multiple times a week across disciplines. ***As a result of our extensive due diligence and joint integration planning, we are now even more confident in the potential of cost savings of this transaction***.

260. This statement was false and misleading when made for the same reasons stated in ¶ 260.

I. March 21, 2016 – Prospectus Containing Letter from Defendant Sorenson to Marriott International Leaders

261. On March 21, 2016, at approximately 1:30 pm EST, Marriott filed a prospectus pursuant to SEC Rule 425 containing a letter from Defendant Sorenson to Marriott International Leaders. In that letter, Defendant Sorenson stated:

> ***Our focus now is to continue the process of integration and complete the closing conditions,*** and we and Starwood believe this revised bid offers the best course for Starwood and Marriott shareholders.

262. This statement was false and misleading when made for the same reasons stated in ¶ 249.

J. March 21, 2016 – Prospectus Containing an Updated Letter to Marriott Associates

263. On March 21, 2016, at approximately 1:30 pm EST, Marriott filed a Prospectus pursuant to SEC Rule 425 containing an updated letter to Marriott associates explaining Marriott's strategy regarding the Merger. In that letter, Defendant Sorenson stated:

> Beyond the math, the strategic story hasn't changed. The simple fact remains that the combination of Marriott and Starwood will create a premier lodging company that will offer broader choice for guests, greater benefits for owners and franchisees, more opportunities for associates and increased value for shareholders of both companies. ***Over the course of the last few months we've had an opportunity to learn even more about Starwood through our integration process and we believe that the benefits of combining both companies are even more compelling than our original expectations.***
>
> * * *
>
> Could Anbang or others still attempt to make another bid for Starwood? Yes, because Starwood is a public company, that's possible and is inherent in the transaction process, but no bids can be made or considered after Starwood's shareholder vote takes place. We've made it clear to Starwood that this offer is aligned with the value we see in Starwood – particularly after months of due diligence through our integration process. The revised agreement includes a break fee of $450 million due to Marriott should Starwood ultimately decide to accept another bid. ***But our focus right now is on continuing the process of integration and completing the closing conditions, and we and Starwood believe this revised bid offers the best course for Starwood and Marriott shareholders.***

264. These statements were false and misleading for the same reasons stated in ¶ 260.

K. March 21, 2016 – Form 8-K

265. On March 21, 2016, after the market closed, Marriott filed an 8-K, signed by Executive VP and General Counsel Edward A. Ryan, which included an amendment to the Merger Agreement and a press release.

266. In that press release, Defendant Sorenson stated:

> ***As a result of extensive due diligence and joint integration planning, Marriott is confident it can achieve $250 million in annual cost synergies within two years after closing, up from $200 million estimated in November 2015 when announcing the original merger agreement.***
>
> ***
>
> ***After five months of extensive due diligence and joint integration planning with Starwood***, including a careful analysis of the brand architecture and future development prospects, we are even more excited about the power of the combined companies and the upside growth opportunities.

267. This statement was false and misleading when made for the same reasons stated in ¶ 260.

L. March 31, 2016 – Press Release from Marriott in Support of the Merger

268. On March 31, 2016, just after the market opened at 9:31 am EST, Marriott issued a press release regarding the upcoming Starwood shareholder vote. In that press release, Defendant Sorenson stated:

> We are focused on maximizing shareholder value and from the beginning of this process we have been steadfast in our belief that a combination with Starwood will offer the highest value to all shareholders. Together, we can provide opportunities for significant equity upside and great long-term value driven by a larger global footprint, wider choice of brands for consumers, substantial synergies, and improved economics to owners and franchisees leading to accelerated global growth and continued strong returns. ***Our integration teams have been diligent in their work over the last few weeks and are more committed than ever to a timely and smooth transition.***

269. This statement was false and misleading when made for the same reasons stated in ¶ 249.

M. April 1, 2016 – Marriott and Starwood M&A Conference Call

270. On April 1, 2016, at 9:00 am EST, Marriott held a conference call to discuss the Merger. On that call, Defendant Sorenson discussed the integration of Starwood's systems. In

response to a question about the integration, Defendant Sorenson touted the extent of the diligence performed:

> Analyst
>
> Good morning, everyone. A quick question on cost synergies. Just wondering if you can provide a little more elaboration on -- the previous estimate was $200 million, it went to $250 million, that is. What was included in the incremental $50 million, and is there any reason to believe that with more information there could be more to come on that front?
>
> Defendant Sorenson
>
> So Tom thought we could do $250 million from the moment we announced a deal. And he knows the cost structure at Starwood, obviously dramatically better than we do. And I guess in a way we just were acknowledging that he was right. ***For us, we want to take it a step at a time and we hadn't, when we announced the deal, really done any organizational diligence, if you will. We've done financial diligence and tried to understand the assets and the balance sheet and those sorts of things.***
>
> ***But in the four months we've had following, we've had -- I think one of our team, the Starwood integration [lead] counted 150-ish meetings between Marriott and Starwood people in various disciplines or various regions around the world, where they are getting to know each other, where they are getting to know the organizations, where they are starting to think about what the combined organization looks like from a staffing level going forward.*** And all of that has given us greater confidence that the $250 million number is achievable. We don't have another number to hang out for you as further upside from that.

271. This statement was false and misleading when made for the same reasons stated in ¶ 260.

N. April 27, 2016 – Form 8-K

272. On April 27, 2016, after the market closed, Marriott filed a Form 8-K that included a press release discussing the Company's earnings and the integration efforts. In that press release, Defendant Sorenson stated:

> Our planned acquisition of Starwood Hotels & Resorts is on track. Shareholders of both companies overwhelmingly approved proposals relating to the merger and we continue to look forward to a mid-2016 closing. ***Toward that end, integration teams from both companies have been working over the last several months to ensure a smooth transition.*** We look forward to creating the largest lodging company in the world.

273. This statement was false and misleading when made for the same reasons stated in ¶ 249.

O. April 28, 2016 – Q1 2016 Form 10-Q

274. On April 28, 2016, at approximately 1:00 pm EST, Marriott filed the Company's Q1 2016 Form 10-Q, which was signed by Defendant Val Bauduin. In the Q1 2016 Form 10-Q, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> *The combined company may not be able to integrate successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized.* ***We entered into the Merger Agreement with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner.***
>
> ***The integration process could also take longer than we anticipate and could result in the loss of valuable employees, the disruption of each company's ongoing businesses, processes and systems or inconsistencies in standards, controls, procedures, practices, policies and compensation arrangements, any of which could adversely affect the combined company's ability to achieve the benefits we anticipate. The combined company's resulting portfolio of approximately 30 brands could be challenging for us to maintain and grow, and the harmonization of our different reservations and other systems and business practices could be more difficult, disruptive, and time consuming than we anticipate. The combined company's results of operations could also be adversely affected by any issues attributable to either company's operations that arise or are based on events or actions that occur before the Starwood Combination closes.*** The

> combined company may also have difficulty addressing possible differences in corporate cultures and management philosophies. The integration process is subject to a number of uncertainties, and we cannot assure you that the benefits we anticipate will be realized at all or as quickly as we expect. If we don't achieve those benefits, our costs could increase, our expected net income could decrease, and the combined company's future business, financial condition, operating results and prospects could suffer.

275. These statements were false and misleading when made for the same reasons stated in ¶ 254.

276. Also in the Q1 2016 Form 10-Q, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Marriott Rewards and The Ritz-Carlton Rewards programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> ***
>
> *We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data*. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches.

***

Any disruption in the functioning of our reservation system, such as in connection with the Starwood Combination, could adversely affect our performance and results. We manage a global reservation system that communicates reservations to our branded hotels that individuals make directly with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel web sites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of

> ***our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of our global reservation system could increase in connection with the system integration that we anticipate undertaking following consummation of the Starwood Combination. Disruptions in or changes to our reservation system could result in a disruption to our business and the loss of important data.***

277. These statements were false and misleading when made for the same reasons stated in ¶ 256.

P. July 28, 2016 – Q2 2016 Earnings Call

278. On July 28, 2016, at 10:00 am EST, Marriott held a conference call to discuss the Q2 2016 earnings, the Merger and integration, and other topics. In his opening remarks, Defendant Sorenson stated:

> I would also like to say that I have never been more proud of Marriott associates. This team has done a lot of transactions over the last five years from the spinoff of Marriott Vacations Worldwide in 2011 to the more recent acquisitions of AC Hotels, Gaylord, Protea and Delta. With each of these transactions, Marriott associates worked hard to first execute the transaction and then capture the strategic value of the deal all while growing and managing our existing business.
>
> The Starwood transaction should be completed in the coming weeks bringing these terrific teams together. ***Both the Marriott and Starwood teams have done exhaustive planning to get ready and we are excited by our prospects.*** While we will see a lot of progress in the near-term, we expect that full integration will be a two-year project.

279. This statement was false and misleading for the same reasons stated in ¶ 260.

Q. July 28, 2016 – Q2 2016 Form 10-Q

280. On July 28, 2016, shortly after noon, Marriott filed the Company's Q2 2016 Form 10-Q, which was signed by Defendant Val Bauduin. In the Q2 2016 Form 10-Q, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> *The combined company may not be able to integrate successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized.* ***We entered into the Merger Agreement with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner.***
>
> ***The integration process could also take longer than we anticipate and could result in the loss of valuable employees, the disruption of each company's ongoing businesses, processes and systems or inconsistencies in standards, controls, procedures, practices, policies and compensation arrangements, any of which could adversely affect the combined company's ability to achieve the benefits we anticipate.*** The combined company's resulting portfolio of approximately 30 brands could be challenging for us to maintain and grow, and the harmonization of our different reservations and other systems and business practices could be more difficult, disruptive, and time consuming than we anticipate. ***The combined company's results of operations could also be adversely affected by any issues attributable to either company's operations that arise or are based on events or actions that occur before the Starwood Combination closes.*** The combined company may also have difficulty addressing possible differences in corporate cultures and management philosophies. ***The integration process is subject to a number of uncertainties, and we cannot assure you that the benefits we anticipate will be realized at all or as quickly as we expect.*** If we do not achieve those benefits, our costs could increase, our expected net income could decrease, and the combined company's future business, financial condition, operating results and prospects could suffer.

281. These statements were false and misleading for the same reasons stated in ¶ 254.

282. Also in the Q2 2016 Form 10-Q, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Marriott Rewards and The Ritz-Carlton Rewards programs, and technologies we make available to our guests. These technologies***

and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.

***

We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our***

> ***reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches.
>
> ***
>
> ***Any disruption in the functioning of our reservation system, such as in connection with the Starwood Combination, could adversely affect our performance and results. We manage a global reservation system that communicates reservations to our branded hotels that individuals make directly with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel web sites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of our global reservation system could increase in connection with the system integration that we anticipate undertaking following consummation of the Starwood Combination. Disruptions in or changes to our reservation system could result in a disruption to our business and the loss of important data.***

283. These statements were false and misleading when made for the same reasons stated in ¶ 256.

R. September 23, 2016 – Marriott to Acquire Starwood M&A Call

284. On September 23, 2016, the day of the Merger closing, Marriott held a conference call to discuss its acquisition of Starwood. On that conference call, Defendant Linnartz discussed the integration efforts:

> I think, as Arne mentioned a moment ago, it was the race to the starting line. We have a lot of work ahead of us on the systems

> front. ***To Arne's point, as we combine systems and get more efficiencies and have more savings, we will not only deliver those savings to our owners, but we'll be able to invest more in consumer-facing technology, things like mobile, et cetera.*** So we're excited that with a bigger platform as a combined Company, we will be able to invest more in consumer-facing technology which is really, really exciting from a consumer standpoint. And again, while we also deliver savings to our owners.

285. The statements concerning the state of the Marriott and Starwood integration were false and misleading when made because they portrayed the integration in a positive light, conveying that the integration would have a minimal impact on Marriott and that Marriott would employ its experience to ensure that the integration would be successful. However, throughout the integration Starwood's guest reservation database was compromised by the Breach. At the time Defendants made these statements, Starwood's IT systems were severely vulnerable, using an outdated Oracle application portal that could not be updated or patched. An adequate merger due diligence process would have easily revealed these glaring and obvious deficiencies, yet Marriott failed to share this important information with the market. In addition to failing to discover the Breach (despite seeing how vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that Defendants failed to address after taking control of the legacy Starwood reservation database including, but not limited to: (1) Starwood's known cybersecurity issues, including a point-of-sale breach announced just five days after the Merger Agreement was signed; (2) significant (and public) intrusions into the systems and databases of Marriott's competitors by hackers to gain access to customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen. Moreover, as confirmed by former employees of Marriott, Defendants failed to spend the money or resources needed to ensure that the transformative Starwood integration was actually

being carried out adequately, and which included operating an IT system that was safe and kept customer data secure.

S. November 7, 2016 – Form 8-K

286. On November 7, 2016, after the market closed, Marriott filed an 8-K signed by Defendant Val Bauduin containing a press release discussing the Company's operations and the integration with Starwood. As to the integration, Defendant Sorenson stated:

> We were thrilled to close the acquisition of Starwood in late September. ***We*** are enthusiastically engaged in welcoming Starwood's associates around the world into the Marriott family and ***are working diligently on integrating the companies and realizing revenue and cost synergies as quickly as possible.***

287. This statement was false and misleading when made for the same reasons stated in ¶ 287.

T. November 9, 2016 – Q3 2016 Form 10-Q

288. On November 9, 2016, at approximately 12:45 pm EST, Marriott filed the Company's Q3 2016 Form 10-Q, which was signed by Defendant Val Bauduin. In the Q3 2016 Form 10-Q, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> *We may not be able to integrate Starwood successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized.* ***We entered into the Merger Agreement with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner.***
>
> ***The integration process could also take longer than we anticipate and could result in the loss of valuable employees, the disruption of each company's ongoing businesses, processes and systems or inconsistencies in standards, controls, procedures, practices, policies and compensation arrangements, any of which could adversely affect the combined company's ability to achieve the***

> ***benefits we anticipate. Our resulting portfolio of approximately 30 brands may be challenging for us to maintain and grow, and the harmonization of our different reservations and other systems and business practices could be more difficult, disruptive, and time consuming than we anticipate.*** We may also have difficulty addressing possible differences in corporate cultures and management philosophies. We may incur unanticipated costs in the integration of the businesses of Starwood. Although we expect that the elimination of certain duplicative costs, as well as the realization of other efficiencies related to the integration of the two businesses, will over time offset the substantial incremental transaction and merger-related costs and charges we incurred in connection with the Starwood Combination, we may not achieve this net benefit in the near term, or at all.
>
> ***The integration process is subject to a number of uncertainties, and we cannot assure you that the benefits we anticipate will be realized at all or as quickly as we expect.*** If we don't achieve those benefits, our costs could increase, our expected net income could decrease, and the combined company's future business, financial condition, operating results, and prospects could suffer.
>
> Our future results will suffer if we do not effectively manage our expanded operations. ***With completion of the Starwood Combination, the size of our business has increased significantly. Our future success depends, in part, upon our ability to manage this expanded business, which poses substantial challenges for management, including challenges related to the management and monitoring of new operations and associated increased costs and complexity.*** We cannot assure you that we will be successful or that we will realize the expected operating efficiencies, cost savings, and other benefits from the combination that we currently anticipate.

289. These statements were false and misleading when made because while warning of potential risks related to integrating the business, Marriott failed to disclose critical facts relevant to these risks. In particular, at the time these statements were made, Starwood's IT systems were severely vulnerable, using an outdated portal and software that could not be updated or patched. The Merger due diligence process (which was severally deficient in and of itself) would have easily revealed these glaring and obvious problems with Starwood's IT department and data security and revealed that there was a dangerous inconsistency in standards and controls (not just

a mere risk), yet Marriott failed to share this important information with the market. In addition to failing to discover the Breach (despite seeing how vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that Defendants failed to address after taking control of the legacy Starwood reservation database including, but not limited to: (1) Starwood's known cybersecurity issues, including a point-of-sale breach announced just five days after the Merger Agreement was signed; (2) significant (and public) intrusions into the systems and databases of Marriott's competitors by hackers to gain access to customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen. Moreover, as confirmed by former employees of Marriott, Defendants failed to spend the money or resources needed to ensure that the transformative Starwood integration was actually being carried out adequately, and which included operating an IT system that was safe and kept customer data secure.

290. Also in the Q3 2016 Form 10-Q, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Marriott Rewards and The Ritz-Carlton Rewards programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> ***
>
> *We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data*. Our

businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the

> future such insurance may not be available to us on commercially reasonable terms.
>
> ***
>
> ***Any disruption in the functioning of our reservation system, such as in connection with our integration of Starwood, could adversely affect our performance and results. We manage a global reservation system that communicates reservations to our branded hotels that individuals make directly with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel websites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of our global reservation system could increase in connection with the system integration that we anticipate undertaking as part of our integration of Starwood. Disruptions in or changes to our reservation system could result in a disruption to our business and the loss of important data.***

291. These statements were false and misleading when made because while warning of potential risks related to cybersecurity, Marriott failed to disclose critical facts relevant to these risks. In particular, at the time these statements were made, Starwood's IT systems were severely vulnerable, using an outdated Oracle application portal that could not be updated or patched. An adequate merger due diligence process would have easily revealed these obvious and glaring deficiencies, yet Marriott failed to share this important information with the market. In addition to failing to discover the Breach (despite seeing how vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that Defendants failed to address after taking control of the legacy Starwood reservation database including, but not limited to: (1) Starwood's known cybersecurity issues, including a point-of-sale breach announced just five days after the Merger Agreement was signed; (2) significant (and public) intrusions into the systems and databases of Marriott's competitors by hackers to gain access to

customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen. Moreover, as confirmed by former employees of Marriott, Defendants failed to spend the money or resources needed to ensure that the transformative Starwood integration was actually being carried out adequately, and which included operating an IT system that was safe and kept customer data secure.

U. February 16, 2017 – Q4 2016 Earnings Conference Call

292. On February 16, 2017, at 3:00 pm EST, Marriott held a conference call to discuss the Company's operations, the integration of Starwood's systems, and other topics. On the topic of integration, in his opening statements Defendant Sorenson stated:

> All in all, ***we are pleased with the pace of integration.*** Our people are working very hard, but they've made amazing progress. I'm incredibly proud of them.
>
> ***The underlying strategy of bringing these two companies together remains sound***, and we are excited about the increasing benefits of the transaction for owners, franchisees, associates, and of course our shareholders. Now, I'd like to turn the call over to Leeny for a review of our financial results and some additional color on the first-quarter and 2017 outlook.

293. This statement was false and misleading when made for the same reasons stated in ¶ 287.

V. February 21, 2017 – 2016 Form 10-K

294. On February 21, 2017, just before the market closed, Marriott filed the Company's Form 10-K for year ending 2016 ("2016 Form 10-K"). The 2016 Form 10-K was signed by Defendants Sorenson, Oberg, and Val Bauduin, and made representations regarding the security of customer data, the Company's operations, the Merger, and other topics.

295. In the 2016 Form 10-K, Marriott stated:

> Keeping pace with developments in technology is important for our operations and our competitive position. Furthermore, ***the***

> ***integrity and protection of customer, employee, and company data is critical to us*** as we use such data for business decisions and to maintain operational efficiency.

296. This statement was false and misleading when made because, while touting how important data security was to Marriott on the one hand, on the other hand, Marriott was failing to perform sufficient due diligence to ensure that customer data purchased from Starwood was protected. At this time, Starwood's guest reservation database was compromised by the Breach. Indeed, at the time they made these statements, Starwood's IT systems were severely vulnerable, using an outdated Oracle application portal that could not be updated or patched. An adequate merger due diligence process would have easily revealed these glaring and obvious deficiencies, yet Marriott failed to share this important information with the market. In additional to failing to discover the Breach (despite seeing how vulnerable Starwood's systems were), Marriott also ignored several red flags in the build-up to the Merger that Defendants failed to address after taking control of the legacy Starwood reservation database including, but not limited to: (1) Starwood's known cybersecurity issues, including a point-of-sale breach announced just five days after the Merger Agreement was signed; (2) significant (and public) intrusions into the systems and databases of Marriott's competitors by hackers to gain access to customer data; and (3) other significant data breaches in other industries where sensitive personal customer data was stolen. Moreover, as confirmed by former employees of Marriott, Defendants failed to spend the money or resources needed to ensure that the transformative Starwood integration was actually being carried out adequately, and which included operating an IT system that was safe and kept customer data secure.

297. Also in the 2016 Form 10-K, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

We may not be able to integrate Starwood successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner, and we cannot assure you that those benefits will be realized at all or as quickly as we expect.*** If we do not achieve those benefits, our costs could increase, our expected net income could decrease, and our future business, financial condition, operating results, and prospects could suffer.

The integration process could take longer than we anticipate and involve unanticipated costs. Disruptions of each company's ongoing businesses, processes, and systems or inconsistencies in standards, controls, procedures, practices, policies, and compensation arrangements could adversely affect the combined company. We may also have difficulty addressing differences in corporate cultures and management philosophies, and in harmonizing our different reservations and other systems and business practices. Although we expect that the elimination of certain duplicative costs, as well as the realization of other efficiencies related to the integration of the two businesses, will over time offset the substantial incremental transaction and merger-related costs and charges we incurred in connection with the Starwood Combination, we may not achieve this net benefit in the near term, or at all.

Our future results will suffer if we do not effectively manage our expanded operations. ***With completion of the Starwood Combination, the size of our business has increased significantly. Our continued success depends, in part, upon our ability to manage this expanded business, which poses substantial challenges for management, including challenges related to the management and monitoring of new operations and associated increased costs and complexity.*** We cannot assure you that we will be successful or that we will realize the expected operating efficiencies, cost savings, and other benefits from the combination that we currently anticipate.

298. These statements were false and misleading when made for the same reasons stated in ¶ 291.

299. Also in the 2016 Form 10-K, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Loyalty Programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> ***
>
> *We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data*. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***
>
> ***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.***

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

***

Any disruption in the functioning of our reservation system, such as in connection with our integration of Starwood, could adversely affect our performance and results. We manage a global reservation system that communicates reservations to our branded hotels that individuals make directly with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel websites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of our global reservation system could increase in connection with the system integration that we anticipate undertaking as part of our integration of Starwood. Disruptions in or changes to our reservation system could result in a disruption to our business and the loss of important data.

300. These statements were false and misleading when made for the same reasons stated in ¶ 293.

W. March 21, 2017 – Form 8-K

301. On March 21, 2017, before the market opened, Marriott filed an 8-K signed by Defendant Val Bauduin containing a press release discussing the integration process. In that press release, Marriott stated: "***Marriott has already made great progress on integrating Starwood***, including immediately linking loyalty programs, integrating its development organization, and rolling out its unified guest feedback system, guestVoice, across legacy-Starwood properties."

302. This statement was false and misleading when made for the same reasons stated in ¶ 287.

X. May 8, 2017 – Form 8-K

303. On May 8, 2017, after the market closed, Marriott filed a Form 8-K signed by Defendant Val Bauduin and attached a press release that discussed the Company's operations and the integration of Starwood's systems. With regard to the integration, Defendant Sorenson stated:

> ***We continue to make great progress on integrating the Starwood and Marriott lodging businesses, gaining efficiencies at both the corporate and property levels.*** Legacy-Starwood hotels are enjoying the benefits of Marriott's OTA contracts and procurement agreements, and are in the process of transitioning to our above-property shared-service model for finance and accounting. Our global sales organization, which maintains relationships with our largest customers, is now fully integrated.

304. This statement was false and misleading when made for the same reasons stated in ¶ 287.

Y. May 9, 2017 – Q1 2017 Form 10-Q

305. On May 9, 2017, just after noon EST, Marriott filed the Company's Q1 2017 Form 10-Q, which was signed by Defendant Val Bauduin. In the Q1 2017 Form 10-Q, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> *We may not be able to integrate Starwood successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized.* ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner, and we cannot assure you that those benefits will be realized at all or as quickly as we expect.*** If we do not achieve those benefits, our costs could increase, our expected net income could decrease, and our future business, financial condition, operating results, and prospects could suffer.
>
> ***The integration process could take longer than we anticipate and involve unanticipated costs. Disruptions of each company's ongoing businesses, processes, and systems or inconsistencies in standards, controls, procedures, practices, policies, and compensation arrangements could adversely affect the combined company. We may also have difficulty addressing differences in corporate cultures and management philosophies, and in harmonizing our different reservations and other systems and business practices.*** Although we expect that the elimination of certain duplicative costs, as well as the realization of other efficiencies related to the integration of the two businesses, will over time offset the substantial incremental transaction and merger-related costs and charges we incurred in connection with the Starwood Combination, we may not achieve this net benefit in the near term, or at all.
>
> *Our future results will suffer if we do not effectively manage our expanded operations.* ***With completion of the Starwood Combination, the size of our business has increased significantly. Our future success depends, in part, upon our ability to manage this expanded business, which poses substantial challenges for management, including challenges related to the management and monitoring of new operations and associated increased costs and complexity.*** We cannot assure you that we will be successful or that we will realize the expected operating efficiencies, cost

> savings, and other benefits from the combination that we currently anticipate.

306. These statements were false and misleading when made for the same reasons stated in ¶ 291.

307. Also in the Q1 2017 Form 10-Q, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Loyalty programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> ***
>
> *We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data*. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***
>
> ***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the***

United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

***

Any disruption in the functioning of our reservation systems, such as in connection with our integration of Starwood, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, or through our telephone call centers, or through intermediaries like travel agents, Internet travel websites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the

> ***functioning of our global reservation systems could increase in connection with the systems integration that we anticipate undertaking as part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

308. These statements were false and misleading when made for the same reasons stated in ¶ 293.

Z. May 9, 2017 – Q1 2017 Earnings Conference Call

309. On May 9, 2017, at 2:00 pm EST, Marriott held a conference call to discuss the Company's operations, the integration of Starwood's systems, and other topics. On that call, Defendant Sorenson again touted the integration of the two systems as a positive. In his opening remarks, Defendant Sorenson stated:

> Demand for our brands remains high, and we are on track to deliver 6% net unit growth in 2017. ***Throughout the company, our teams are making tremendous progress on the Starwood integration.*** We've already the transitioned HR systems for Starwood hotels in the U.S. and expect other continents will follow later in 2017. In March, we added 36,000 associates to the Marriott payroll system. For our guests, all our hotels worldwide are now on an integrated system for guest event and social media feedback. This summer, we expect to publish harmonized global brand standards which, along with regular audits, is an essential step in establishing property accountability and maintaining guest satisfaction.

310. This statement was false and misleading when made for the same reasons stated in ¶ 287.

AA. August 7, 2017 – Form 8-K

311. On August 7, 2017, after the market closed, Marriott filed a Form 8-K signed by Defendant Val Bauduin and attached a press release discussing the Company's operations, the integration of Starwood's systems, and other topics. In that press release, in discussing the

integration of Starwood's systems, Defendant Sorenson stated: "***Integration of the Starwood transaction is on track.***"

312. These statements were false and misleading when made for the same reasons stated in ¶ 287. Additionally, Defendants' statement was one of present fact on the progress of the integration that was both objectively and subjectively false when made.

BB. August 8, 2017 – Q2 2017 Form 10-Q

313. On August 8, 2017, at approximately 2:25 pm EST, Marriott filed the Company's Q2 2017 Form 10-Q, which was signed by Defendant Val Bauduin. In the Q2 2017 Form 10-Q, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> *We may not be able to integrate Starwood successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized.* ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner, and we cannot assure you that those benefits will be realized as fully or as quickly as we expect.*** If we do not achieve those benefits, our costs could increase, our expected net income could decrease, and our future business, financial condition, operating results, and prospects could suffer.
>
> ***The integration process could take longer than we anticipate and involve unanticipated costs. Disruptions of each company's ongoing businesses, processes, and systems or inconsistencies in standards, controls, procedures, practices, policies, and compensation arrangements could adversely affect the combined company. We may also have difficulty addressing differences in corporate cultures and management philosophies, and in harmonizing our different reservations and other systems and business practices.*** Although we expect that the elimination of certain duplicative costs, as well as the realization of other efficiencies related to the integration of the two businesses, will over time offset the substantial incremental transaction and merger-related costs and charges we incurred in connection with

> the Starwood Combination, we may not achieve this net benefit in the near term, or at all.
>
> *Our future results will suffer if we do not effectively manage our expanded operations.* ***With completion of the Starwood Combination, the size of our business increased significantly. Our future success depends, in part, upon our ability to manage this expanded business, which poses substantial challenges for management, including challenges related to the management and monitoring of new operations and associated increased costs and complexity.*** We cannot assure you that we will be successful or that we will realize the expected operating efficiencies, cost savings, and other benefits from the combination that we currently anticipate.

314. These statements were false and misleading when made for the same reasons stated in ¶ 291.

315. Also in the Q2 2017 Form 10-Q, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Loyalty Programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> ***
>
> *We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data*. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers,

in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have increased significantly in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

***

> ***Any disruption in the functioning of our reservation systems, such as in connection with our integration of Starwood, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, or through our telephone call centers, or through intermediaries like travel agents, Internet travel websites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase in connection with the systems integration that we anticipate undertaking as part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

316. These statements were false and misleading for the same reasons stated in ¶ 293.

CC. October 5, 2017 – Privacy Statement

317. On September 23, 2016, Marriott completed the acquisition of Starwood. On October 5, 2017, Marriott updated the Online Privacy Statement it presented to the public from the start of the Class Period until around February 2018 on starwoodhotels.com. In that statement, Marriott informed the public of its policy for transferring, storing, and securing the customer data the Company collected through starwoodhotels.com:

> SAFE HARBOR
>
> In addition, Starwood is certified under the Safe Harbor privacy framework as set forth by the U.S. Department of Commerce, European Commission and Switzerland regarding the collection, storage, use, transfer and other processing of PII transferred from the European Economic Area or Switzerland to the U.S. Please note that since October 6, 2015, the European Union no longer recognizes Safe Harbor. ***Nonetheless, Starwood upholds to comply with the Safe Harbor Privacy Principles.***
>
> SECURITY SAFEGUARDS

> ***Starwood recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your personal data against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. Although "guaranteed security" does not exist either on or off the Internet, we safeguard your information using appropriate administrative, procedural and technical safeguards, including password controls, "firewalls" and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit.***

318. These statements were false and misleading when made for the same reasons stated in ¶ 298. Additionally, Marriott was in violation of the Safe Harbor Principles the Company stated it complied with due to the Company's failure to conduct adequate due diligence during the Merger, failure to detect the Breach in the legacy Starwood guest reservation database, and failure to maintain adequate security measures to protect customer data while operating that breached database for nearly two years after acquiring it from Starwood in the Merger.

DD. November 7, 2017 – Form 8-K

319. On November 7, 2017, after the market closed, Marriott filed a Form 8-K signed by Defendant Val Bauduin and attached a press release discussing the Company's operations, the integration of Starwood's systems, and other topics. In the press release Defendant Sorenson stated:

> It's been just over a year since the completion of the Starwood acquisition. ***We are pleased with our progress on the integration.*** Our properties and general and administrative functions have already realized meaningful cost savings. From the date of the acquisition through last week, we have recycled assets totaling more than $1.1 billion of our $1.5 billion goal. Year-to-date through November 7, we have already returned $2.7 billion to

> shareholders through dividends and share repurchase and believe we could return nearly $3.5 billion in 2017.

320. This statement was false and misleading when made for the same reasons stated in ¶ 287.

EE. November 8, 2017 – Q3 2017 Form 10-Q

321. On November 8, 2017, at just after 1:30 pm EST, Marriott filed the Company's Q3 2017 Form 10-Q, which was signed by Defendant Val Bauduin. At the time of the filing of the Q3 2017 Form 10-Q, the Merger had already closed and Marriott owned the legacy Starwood's guest reservation database.

322. In the Q3 2017 Form 10-Q, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> *Some of the anticipated benefits of combining Starwood and Marriott may still not be realized.* ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to a number of uncertainties, including whether we can continue to integrate the business of Starwood in an efficient and effective manner and whether, and on what terms, we can reach agreement with the companies that issue our branded credit cards and the timeshare companies with whom we do business to allow us to move to a single unified reservation system and loyalty platform.***
>
> ***The integration process could take longer than we anticipate and involve unanticipated costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We also may still encounter difficulties harmonizing our different reservations and other systems and business practices as the integration process continues.*** As a result of these or other factors, we cannot assure you when or that we will be able to fully realize additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits.

323. These statements were false and misleading when made for the same reasons stated in ¶ 291.

324. Also in the Q3 2017 Form 10-Q, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Loyalty Programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> ***
>
> *We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data*. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***
>
> ***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to***

satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have increased significantly in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

***

Any disruption in the functioning of our reservation systems, such as in connection with our integration of Starwood, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, or through our telephone call centers, or through intermediaries like travel agents, Internet travel websites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase in connection with the systems integration that we anticipate

> ***undertaking as part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

325. These statements were false and misleading when made for the same reasons stated in ¶ 293.

FF. November 8, 2017 – Q3 2017 Earnings Call

326. On November 8, 2017, at 3:00 pm EST, Marriott held a conference call to discuss the Company's operations, the integration of Starwood's systems, and other topics. In his opening remarks, Defendant Sorenson stated:

> We've never been more optimistic about our business, our underlying competitive strengths and our long-term growth potential. ***The Starwood integration is on track.*** We have identified more synergies and more business opportunities than we anticipated. We continue to believe we will achieve $250 million of G&A savings and expect to do that in 2018. And we continue to improve our products, services and systems to enhance the value of every room night.

327. This statement was false and misleading when made for the same reasons stated in ¶ 287. Additionally, Defendants' statement was one of present fact on the progress of the integration that was both objectively and subjectively false when made.

GG. January 12, 2018 – Hoffmeister Interview

328. On January 12, 2018, Defendant Hoffmeister conducted an interview with Rich Siegel to discuss the Merger, and other topics. In that interview, Defendant Hoffmeister was asked about the integration process, and in response misleadingly stated that Marriott was utilizing the "***best***" of Starwood's systems and that Marriott had conducted a "thorough analysis" of Starwood's systems:

> Siegel
>
> It's been more than a year since Marriott International merged with Starwood. From your perspective, how's the integration process going?
>
> Defendant Hoffmeister
>
> Whenever two large companies come together, you have to determine what processes, systems and tools to use. ***We're going through the process of bringing our systems together to get the best of both worlds wherever possible.*** It's very exciting. We have a lot going on, and a lot of work ahead still, but it's a very exciting time.
>
> ***
>
> Siegel
>
> At the Download conference, you mentioned that when you learned of the Starwood merger, as CIO you looked for advice from other ICOs. Can you elaborate on that?
>
> Defendant Hoffmeister
>
> ***
>
> Two themes emerged. The first was quite simply to "just adopt and go." Choose your systems and just go with them; you're not going to please everyone. ***We did a thorough analysis of the systems before we made our decision***, but we didn't dwell on it, we just made a decision.

329. These statements were false and misleading when made for the reasons in ¶ 287.

HH. February 14, 2018 – 2017 Form 10-K

330. Marriott filed its Form 10-K for year ending 2017 ("2017 Form 10-K") just before the market closed on February 15, 2018. The 2017 Form 10-K was signed by Defendants Sorenson, Oberg, and Val Bauduin, and made representations regarding the security of customer data, the Company's operations, the integration of Starwood's systems, and other topics.

331. In the 2017 Form 10-K, Marriott stated:

> Keeping pace with developments in technology is important for our operations and our competitive position. Furthermore, ***the integrity and protection of customer, employee, and company data is critical to us*** as we use such data for business decisions and to maintain operational efficiency.

332. This statement was false and misleading when made for the same reasons stated in ¶ 298.

333. Also in the 2017 Form 10-K, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> *Some of the anticipated benefits of combining Starwood and Marriott may still not be realized.* ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to several uncertainties, including whether we can continue to effectively and efficiently integrate the Starwood business and whether, and on what terms, we can reach agreement with the timeshare companies with whom we do business to allow us to move to a single unified reservation system and loyalty platform.***
>
> ***Integration could also take longer than we anticipate and involve unexpected costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We also may still encounter difficulties harmonizing our different reservations and other systems and business practices as the integration process continues.*** Because of these or other factors, we cannot assure you when or that we will be able to fully realize additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits.

334. These statements were false and misleading when made for the same reasons stated in ¶ 291.

335. Also in the 2017 Form 10-K, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging***

industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, property management, human resources and payroll systems, our Loyalty Programs, and technologies we make available to our guests and for our associates. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and our business could suffer if we cannot do that as quickly or effectively as our competitors or within budgeted costs and time frames. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.

***

We are exposed to risks and costs associated with protecting the integrity and security of company associate and guest data. Our businesses process, use, and transmit large volumes of associate and guest data, including credit card numbers and other personal information in various information systems that we maintain and in systems maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that guest, associate, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

Our guests and associates also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by laws and governmental regulation and the requirements of the payment card industry are also increasingly demanding, in the U.S., the European Union, Asia, and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing legal and regulatory requirements and employee and guest expectations, or may require significant additional investments or time to do so.

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our information systems

> ***and records and those of our owners, franchisees, licensees, or service providers.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of guest, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, that insurance coverage may not be sufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.
>
> ***
>
> ***Any disruption in the functioning of our reservation systems, as part of our integration of Starwood or otherwise, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, through our telephone call centers, or through intermediaries like travel agents, Internet travel websites, and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase with the anticipated systems integration that is part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

336. These statements were false and misleading when made for the same reasons stated in ¶ 293.

II. May 9, 2018 – Q1 2018 Earnings Conference Call

337. On May 9, 2018, Marriott held a conference to discuss the Company's operations, the integration of Starwood's systems, and other topics. In response to a question about the integration of Starwood's systems, Defendant Sorenson touted the "***great progress***" that Marriott had made.

> ***We continue to make great progress in our integration of Starwood.*** Thus far in 2018, we have combined financial reporting systems, integrated our North American sales organization and recycled approximately $170 million in capital from asset sales and loan repayments. By August, we expect guests will be able to see and book all of our inventory on each of our Marriott and Starwood websites and apps and enjoy our unified loyalty programs.

338. This statement was false and misleading when made for the same reasons stated in ¶ 287.

JJ. May 10, 2018 – Q1 2018 Form 10-Q

339. On May 10, 2018, shortly after the market opened, Marriott filed the Company's Q1 2018 Form 10-Q, which was signed by Defendant Val Bauduin. In the Q1 2018 Form 10-Q, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> *Some of the anticipated benefits of combining Starwood and Marriott may still not be realized.* ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to several uncertainties, including whether we can continue to effectively and efficiently integrate the Starwood business.***
>
> ***Integration could also take longer than we anticipate and involve unexpected costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We also may still encounter difficulties harmonizing our different reservations and other systems,***

> ***Loyalty Programs and other business practices as the integration process continues.*** Because of these or other factors, we cannot assure you when or that we will be able to fully realize additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits, or that difficulties encountered with our harmonization efforts will not have adverse effects on our business or reputation.

340. These statements were false and misleading when made for the same reasons stated in ¶ 291.

341. Also in the Q1 2018 Form 10-Q, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, property management, human resources and payroll systems, our Loyalty Programs, and technologies we make available to our guests and for our associates. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and our business could suffer if we cannot do that as quickly or effectively as our competitors or within budgeted costs and time frames. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> ***
>
> *We are exposed to risks and costs associated with protecting the integrity and security of company, employee, and guest data.* Our businesses process, use, and transmit large volumes of employee and guest data, including credit card numbers and other personal information in various information systems that we maintain and in systems maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that guest, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

Our guests and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by laws and governmental regulation and the requirements of the payment card industry are also increasingly demanding, in the U.S., the European Union, Asia, and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing legal and regulatory requirements and employee and guest expectations, or may require significant additional investments or time to do so.

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our information systems and records and those of our owners, franchisees, licensees, or service providers. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of guest, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits, and negative publicity, resulting in tangible adverse effects on our business, including consumer boycotts, lost sales, litigation, loss of development opportunities, or associate retention and recruiting difficulties, all of which could affect our market share, reputation, business, financial condition, or results of operations. The techniques used to obtain unauthorized access, disable or degrade service, or sabotage information systems change frequently, can be difficult to detect for long periods of time, and can be difficult to assess ore remediate even once detected, which could magnify the severity of these adverse effects.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, that insurance coverage may not be sufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related

> breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.
>
> ***
>
> ***Any disruption in the functioning of our reservation systems, as part of our integration of Starwood or otherwise, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, through our telephone call centers, or through intermediaries like travel agents, Internet travel websites, and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase with the anticipated systems integration that is part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

342. These statements were false and misleading when made for the same reasons stated in ¶ 293.

KK. August 7, 2018 – Q2 2018 Form 10-Q

343. On August 7, 2018, shortly before noon EST, Marriott filed the Company's Q2 2018 Form 10-Q, which was signed by Defendant Val Bauduin. In the Q2 2018 Form 10-Q, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> *Some of the anticipated benefits of combining Starwood and Marriott may still not be realized.* ***We decided to acquire Starwood with the expectation that the Starwood Combination would result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to several uncertainties, including whether we can continue to effectively and efficiently integrate the Starwood business.***

> ***Integration could also take longer than we anticipate and involve unexpected costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We also may still encounter difficulties harmonizing our different reservations and other systems, Loyalty Programs and other business practices as the integration process continues.*** Because of these or other factors, we cannot assure you when or that we will be able to fully realize additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits, or that difficulties encountered with our harmonization efforts will not have adverse effects on our business or reputation.

344. These statements were false and misleading when made for the same reasons stated in ¶ 291.

345. Also in the 2017 Form 10-K, when describing **potential** risks the Company **might** face as a result of its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, property management, human resources and payroll systems, our Loyalty Programs, and technologies we make available to our guests and for our associates. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and our business could suffer if we cannot do that as quickly or effectively as our competitors or within budgeted costs and time frames. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> ***
>
> *We are exposed to risks and costs associated with protecting the integrity and security of company, employee, and guest data.* Our businesses process, use, and transmit large volumes of employee and guest data, including credit card numbers and other personal information in various information systems that we maintain and in systems maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas

such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that guest, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

Our guests and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by laws and governmental regulation and the requirements of the payment card industry are also increasingly demanding, in the U.S., the European Union, Asia, and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing legal and regulatory requirements and associate and guest expectations, or may require significant additional investments or time to do so.

Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our information systems and records and those of our owners, franchisees, licensees, or service providers. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of guest, associate, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits, and negative publicity, resulting in tangible adverse effects on our business, including consumer boycotts, lost sales, litigation, loss of development opportunities, or associate retention and recruiting difficulties, all of which could affect our market share, reputation, business, financial condition, or results of operations. The techniques used to obtain unauthorized access, disable or degrade service, or sabotage information systems change frequently, can be difficult to detect for long periods of time, and can be difficult to assess ore remediate even once detected, which could magnify the severity of these adverse***

> ***effects.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, that insurance coverage may not be sufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.
>
> ***
>
> ***Any disruption in the functioning of our reservation systems, as part of our integration of Starwood or otherwise, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, through our telephone call centers, or through intermediaries like travel agents, Internet travel websites, and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase with the anticipated systems integration that is part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

346. These statements were false and misleading when made for the same reasons stated in ¶ 293.

LL. August 15, 2018 – Privacy Statement

347. As of August 15, 2018, Marriott provided the public with a Global Privacy Statement, which was last updated on May 5, 2018. The Global Privacy Statement applied to both Marriott, its wholly-owned subsidiary Starwood, and Marriott's affiliates. In the Global Privacy Statement, Marriott provided the public with its policies and procedures for using, collecting, and storing the data the Company collects from its customers.

> Security
>
> ***We seek to use reasonable organizational, technical and administrative measures to protect Personal Data.*** Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the *"Contacting Us"* section, below.
>
> Privacy Shield Certified
>
> ***Marriott International, Inc. and certain of its U.S. affiliates have certified to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks.*** Our certifications can be found at: www.privacyshield.gov/list. For more information about the Privacy Shield principles, please visit: www.privacyshield.gov. Our Privacy Shield Guest Privacy Policy can be found here.

348. These statements were false and misleading when made for the reasons in ¶ 298. Additionally, Marriott was in violation of the Privacy Shield Frameworks the Company stated it complied with due to the Company's failure to conduct adequate due diligence during the Merger, failure to detect the Breach in the legacy Starwood guest reservation database, and failure to maintain adequate security measures to protect customer data while operating that breached database for nearly two years after acquiring it from Starwood in the Merger.

MM. October 20, 2018 – Interview with Richmond Times Dispatch

349. In an article in the New York Times titled *Marriott's Merger of Hotel Rewards Programs Tests Members' Loyalty*, Marriott's Senior VP of Global Loyalty David Flueck gave an interview to the Richmond Times Dispatch. In that article, Mr. Flueck "***described the merger as 99.9 percent successful***, though he acknowledged that it still left millions of customer records in limbo, some for weeks before they were resolved."

350. This statement was false and misleading when made because it omitted the fact that Defendants had actual knowledge that the legacy Starwood guest reservation database had

been breached. By this time, Marriott had actual knowledge of the Breach, including that the attackers had used a RAT and Mimikatz as a part of their infiltration of the database. Additionally, this statement was false and misleading for all the reasons stated in ¶ 287.

NN. November 5, 2018 – Form 8-K

351. On November 5, 2018, after the market closed, Marriott filed a Form 8-K signed by Defendant Val Bauduin and attached a press release discussing the Company's operations, the integration of Starwood's systems, and other topics. In regards to the integration of Starwood's system, Defendant Sorenson stated:

> It's been just over two years since the completion of the Starwood acquisition. ***We are in the home stretch on integrating the companies and are pleased with the results.***

352. This statement was false and misleading when made because it omitted the fact that Defendants had actual knowledge that the legacy Starwood guest reservation database had been breached. By this time, Marriott had actual knowledge of the Breach, including that the attackers had used a RAT and Mimikatz as a part of their infiltration of the database. Additionally, the statement was false and misleading for all the reasons stated in ¶ 287.

OO. November 6, 2018 – Q3 2018 Form 10-Q

353. On November 6, 2018, shortly before noon, Marriott filed the Company's Q3 2018 Form 10-Q, which was signed by Defendant Val Bauduin.

354. Also in the Q3 2018 Form 10-Q, when describing **potential** risks the Company **might** face as a result of the Merger, Marriott stated:

> *Some of the anticipated benefits of combining Starwood and Marriott may still not be realized.* ***We decided to acquire Starwood with the expectation that the Starwood Combination would result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to***

> ***several uncertainties, including whether we can continue to effectively and efficiently integrate the Starwood business.***
>
> ***Integration could also take longer than we anticipate and involve unexpected costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We have encountered challenges in harmonizing our different reservations and other systems, Loyalty Program, and other business practices, and may encounter additional or increased challenges as the integration process continues.*** Because of these or other factors, we cannot assure you when or that we will be able to fully realize additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits, or that challenges encountered with our harmonization efforts will not have adverse effects on our business or reputation.

355. These statements were false and misleading because while warning of potential risks related to cybersecurity, Marriott failed to disclose critical facts relevant to these risks including the fact that Defendants had actual knowledge that the legacy Starwood guest reservation database had been breached. By this time, Marriott had actual knowledge of the Breach, including that the attackers had used a RAT and Mimikatz as a part of their infiltration of the database. Additionally, this statement was false and misleading for all the reasons stated in ¶ 291.

356. Also in the Q3 2018 Form 10-Q, when describing **potential** risks the Company **might** face in its technology and information protection operations, Marriott stated:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, property management, human resources and payroll systems, our Loyalty Program, and technologies we make available to our guests and for our associates. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and our business could suffer if we cannot do that as quickly or effectively as our competitors or within budgeted costs and time frames. We also***

may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.

***

We are exposed to risks and costs associated with protecting the integrity and security of company, associate, and guest data. In the operation of our business, we collect, store, use, and transmit large volumes of data regarding associates, guests, customers, owners, licensees, franchisees, and our own business operations, including credit card numbers, reservation and loyalty data, and other personal information, in various information systems that we maintain and in systems maintained by third parties, including our owners, franchisees, licensees, and service providers. ***The integrity and protection of this data is critical to our business. If this data is inaccurate or incomplete, we could make faulty decisions.***

Our guests and associates also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect and appropriately use their personal information. The information, security, and privacy requirements imposed by laws and governmental regulation, our contractual obligations, and the requirements of the payment card industry are also increasingly demanding in the U.S., the European Union, Asia, and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing legal and regulatory requirements and associate and guest expectations, or may require significant additional investments or time to do so. We may incur significant additional costs to meet these requirements, obligations, and expectations, and in the event of alleged or actual noncompliance we may experience increased operating costs, increased exposure to fines and litigation, and increased risk of damage to our reputation and brand.

***

Cyber security incidents could have a disruptive effect on our business. We have implemented security measures to safeguard our systems and data, and we may implement additional measures in the future, but our measures or the measures of our service providers or our owners, franchisees, licensees, and their service providers may not be sufficient to maintain the confidentiality, security, or availability of the data we collect,

store, and use to operate our business. Efforts to hack or circumvent security measures, efforts to gain unauthorized access to data, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, "phishing" or other types of business email compromises, operator error, or inadvertent releases of data may materially impact our information systems and records and those of our owners, franchisees, licensees, or service providers. Our reliance on computer, Internet-based, and mobile systems and communications and the frequency and sophistication of efforts by third parties to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years. Like most large multinational corporations, we have experienced cyber-attacks, attempts to disrupt access to our systems and data, and attempts to affect the integrity of our data, and the frequency and sophistication of such efforts could continue to increase. Although some of these efforts may not be successful or impactful, a significant theft, loss, loss of access to, or fraudulent use of guest, associate, owner, franchisee, licensee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Depending on the nature and scope of the event, compromises in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits, and negative publicity, resulting in tangible adverse effects on our business, including consumer boycotts, lost sales, litigation, loss of development opportunities, or associate retention and recruiting difficulties, all of which could affect our market share, reputation, business, financial condition, or results of operations. The techniques used to obtain unauthorized access, disable or degrade service, or sabotage information systems change frequently, can be difficult to detect for long periods of time, and can involve difficult or prolonged assessment or remediation periods even once detected, which could magnify the severity of these adverse effects. In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, that insurance coverage may not be sufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security compromises, and other related incidents. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

Any disruption in the functioning of our reservation systems, as part of our integration of Starwood or otherwise, could adversely

> ***affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, through our telephone call centers, or through intermediaries like travel agents, Internet travel websites, and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase with the ongoing systems integration that is part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

357. These statements were false and misleading because while warning of potential risks related to cybersecurity, Marriott failed to disclose critical facts relevant to these risks including the fact that Defendants had actual knowledge that the legacy Starwood guest reservation database had been breached. By this time, Marriott had actual knowledge of the Breach, including that the attackers had used a RAT and Mimikatz as a part of their infiltration of the database. Additionally, this statement was false and misleading for all the reasons stated in ¶ 291.

VIII. ADDITIONAL ALLEGATIONS SUPPORTING SCIENTER

358. As described below, the Individual Defendants had actual knowledge that the statements and omissions made by them were false and misleading, or acted with severely reckless disregard as to the truth or falsity of those statements and omissions. The Individual Defendants' knowledge of, or severely reckless disregard for, the truth is demonstrated by admissions and substantial direct and circumstantial evidence supporting a strong inference of scienter.

A. Customers and Customer Data Are a Core Part of Marriott's Operations

359. A hotel is not really a hotel if it does not have any guests. Marriott relies on guest data to bring guests to the Company's hotels and needs its reservation systems to logistically sign guests up for their rooms and obtain payment information for the rooms. Once those guests are in the hotel, Marriott continues to earn revenues in the form of food and beverage sales. As a hotel business, there is no part of Marriott's operations that was not affected by, or connected to, customer reservations and the data those customers provide.

360. Defendants Sorenson and Oberg, among other Marriott executives, repeatedly made public statements about the importance of customer data to the Merger and Marriott's operations generally. Additionally, Marriott engaged in strategic partnerships with third parties with the sole purpose of sharing the personal information of its customers.

361. One of Defendants' primary drivers in executing a transformational transaction like the Merger was Starwood's customer data. As a result, Defendants' due diligence should have been heightened and focused on the guest reservation database. Defendants executed a $13 billion acquisition, the largest transaction in the Company's history, to gain access to Starwood's customers and their personal data. At the announcement of the Merger, analysts and news outlets commented on the importance of Starwood's customer data to Marriott. Accordingly, the Individual Defendants needed to focus on ensuring the integration of the systems of the two companies was a success and that the most important asset in the transaction – customer data – was secure.

362. That the Breach affected the Company's guest reservation database and customer data, a part of Marriott's core operations, supports a strong inference of scienter.

B. Individual Defendants Knew or Were at Least Severely Reckless in Not Knowing that Marriott's Merger Diligence Was Inadequate

363. The Individual Defendants made statements about the due diligence process for the most important merger the Company had ever attempted, so they were charged with knowing whether the due diligence process was actually being performed adequately. They were also required to employ basic due diligence processes to ensure the quality of the customer data, and security and IT operations they were purchasing. The ICO found that Marriott's due diligence process during the Merger was not adequate and this is borne out by the nature of the cyberattack, the glaring and obvious vulnerabilities of the Starwood system, and the opportunities Marriott had to discover or remedy these vulnerabilities over the course of several years.

364. The Individual Defendants knew, or were at least severely reckless in not knowing, of numerous red flags prior to executing the Merger including, but not limited to: (1) the poor quality of Starwood's IT systems generally; (2) Starwood's known cybersecurity issues and prior hacks, including a point-of-sale breach announced just five days after the Merger Agreement was signed; (3) significant intrusions into the databases of Marriott's competitors by hackers to gain access to customer data; and (4) other significant data breaches in other industries where sensitive personal customer data was available.

365. As a result of these "red flags," the Individual Defendants knew, or were at least severely reckless in not knowing, that Marriott needed to perform heightened due diligence on Starwood's systems. Instead, Marriott's due diligence was woefully inadequate. According to Defendant Sorenson, Marriott "hadn't, when [the Company] announced the deal, really done any organizational diligence." Marriott's lax attitude towards security continued after the signing of

the Merger Agreement until the closing of the Merger, despite Marriott's repeated representations to the market to the contrary, as detailed in Section VI(C)(2)(a).

C. Individual Defendants Failed to Detect the Breach for Approximately Two Years Despite Obvious Flaws in Starwood's System

366. For nearly two years, Marriott deliberately, or at least severely recklessly, failed to perform adequate tests on the obviously vulnerable legacy Starwood guest reservation database. As explained by numerous former employees of Marriott and Starwood, it was clear that Marriott was subsuming a company with glaring flaws in its IT systems. Moreover, the market was also shocked that Marriott failed to detect this intrusion for two years after the acquisition – precisely because the expectation was that if Marriott had been conducting the vulnerability scans and testing it was required to do, it would have seen and safeguarded these vulnerabilities.

D. Defendant Sorenson Admittedly Had Actual Knowledge of the Breach More Than Two Months Before Informing the Public

367. According to congressional testimony from Defendant Sorenson, he had actual knowledge of the Breach of the legacy Starwood guest reservation database by September 17, 2018. That Defendants continued to make representations to the market describing a hack as a "risk" when they knew it had actually come to pass, supports a strong inference of scienter. Additionally, that Defendants continued to make statements touting the progress of the integration while possessing actual knowledge that a key part of that integration had been disrupted by the second largest data breach in history supports a strong inference of scienter.

E. Defendant Sorenson was "Hands On" with Marriott's M&A Activity, and M&A Due Diligence Standards Support He Would Have Been Involved in Due Diligence

368. Defendant Sorenson was "hands on" when it came to Marriott's M&A activity. Prior to joining Marriott, Defendant Sorenson was an M&A partner with Latham & Watkins.

His relationship with Marriott began more than 25 years ago when Defendant Sorenson represented the Company regarding acquisitions it made. Defendant Sorenson joined Marriott as the head of the Company's M&A activity in 1996 and promptly undertook his first acquisition with the Company by acquiring Renaissance Hotels. As noted by Defendant Linnartz, Defendant Sorenson is Marriott's "M&A guy."

369. Defendant Sorenson was personally involved with Marriott's acquisition of Starwood. Defendant Sorenson was Marriott's point person during Marriott's initial interest in Starwood, Marriott's decision to reengage with the acquisition process, and Marriott's ultimate decision to acquire Starwood. As detailed in prospectuses filed related to the Merger, Defendant Sorenson held numerous individual meetings with Starwood executives during the acquisition process. Additionally, Defendant Sorenson was a member of the Board and met repeatedly with the Company's Board to keep them informed of the process. The Prospectus also states that the Board, of which Defendant Sorenson was a member gained an enhanced "understanding of the integration process" with the addition of the former Starwood board members. The Prospectus also stated that the Board's review of the due diligence process gave it a "favorable" outlook for the Merger. Finally, based on the due diligence standards in the RACI matrix, at least Defendants Sorenson and Hoffmeister would have been intimately involved in the due diligence process and should have discovered the glaring issues with Starwood's protection of customer data.

F. The Other Individual Defendants Acted with Scienter

370. As Marriott's CIO, Defendant Hoffmeister was deeply involved in the Merger. According to CW 1, Defendant Hoffmeister ran the entire IT organization throughout the process. Additionally, CW 6 said that Defendant Hoffmeister was involved in presenting the IT budget to Defendant Sorenson. Given his involvement in the Merger and integration process,

Defendant Hoffmeister knew that Marriott had not performed adequate diligence, nor performed adequate security during the integration, and made false and misleading statements to the contrary. Defendant Hoffmeister was at least severely reckless in not knowing whether Marriott had actually performed adequate diligence or performed adequate security checks and making false and misleading statements on the subject anyway.

371. According to Defendant Linnartz's biography on Marriott's website, she is responsible for "information technology worldwide." Additionally, Defendant Linnartz gave interviews and made appearances at various conferences throughout the Class Period acknowledging the importance of Starwood's data and technology generally to Marriott's operations. Further, Defendant Linnartz often discussed the importance of integrating the loyalty programs of Starwood and Marriott. Defendant Linnartz knew Marriott was not paying adequate attention to security during the integration and made statements to the contrary. Defendant Linnartz was at least severely reckless in not knowing whether Marriott had performed adequate security checks and making false and misleading statements on the subject anyway.

372. In addition to signing the Company's SEC filings, Defendants Oberg and Val Bauduin were each named Manager of Starwood upon the closing of the Merger. As Managers of the newly acquired entity, Defendants Oberg and Val Bauduin would have been intricately involved in the integration process. Given each of their involvement in both the Merger and integration process, Defendants Oberg and Val Bauduin each knew that Marriott had not performed adequate diligence, nor performed adequate security during the integration, and made false and misleading statements to the contrary. Defendants Oberg and Val Bauduin were at least severely reckless in not knowing whether Marriott had actually performed adequate

diligence or performed adequate security checks and making false and misleading statements on the subject anyway.

IX. LOSS CAUSATION

373. During the Class Period, as detailed herein, Defendants engaged in a scheme to deceive the market and a course of conduct that artificially inflated the price of Marriott's securities and operated as a fraud or deceit on Class Period purchasers of Marriott's securities by failing to disclose and misrepresenting the adverse facts detailed herein. Later, when Defendants' prior misrepresentations and fraudulent course of conduct were revealed to the market, the price of Marriott's securities declined significantly as the prior artificial inflation was released from the Company's stock price.

374. As a result of their purchases of Marriott's securities during the Class Period, Lead Plaintiff and the other Class members suffered economic loss, *i.e.*, damages, under the federal securities laws. Defendants' false and misleading statements had the intended effect and caused Marriott's securities to trade at artificially inflated levels throughout the Class Period, closing as high as $147.99 on January 29, 2018.

375. By concealing from investors the adverse facts detailed herein, Defendants presented a misleading picture of Marriott's business and prospects. When Defendants revealed these adverse facts to the market, the price of Marriott's securities fell dramatically. This decline removed the artificial inflation from the price of Marriott's securities, causing economic loss to investors who had purchased Marriott's securities during the Class Period.

376. The decline in the price of Marriott's securities following the revelations on November 30, 2018, was a direct result of the nature and extent of Defendants' fraudulent misrepresentations being revealed to investors and the market. The timing and magnitude of the price declines in Marriott's securities, Defendants' post Class Period revelations, and analyst

reactions to the news, individually and collectively, negate any inference that the loss suffered by Lead Plaintiff and the other Class members was caused by changed market conditions, macroeconomic or industry factors, or Company-specific facts unrelated to Defendants' fraudulent conduct.

377. The economic loss, *i.e.*, damages, suffered by Lead Plaintiff and the other Class members was a direct result of Defendants' fraudulent scheme and course of conduct to artificially inflate the price of Marriott's securities and the subsequent material decline in the value of Marriott's securities when Defendants' prior misrepresentations, misleading half-truths and other fraudulent conduct were revealed.

378. Specifically, on November 30, 2018, Defendants revealed that legacy Starwood's guest reservation database that Marriott owned and operated had been compromised by a breach since at least a year before Marriott acquired it. On November 30, 2018, the Company revealed that the sensitive, personal information of approximately 500 million guests had been stolen from Marriott's customers through the Breach in the legacy Starwood guest reservation database. The Company revealed that attackers had stolen; (1) names; (2) passport numbers; (3) dates of birth; (4) credit card information; (5) home address; and (6) other valuable, sensitive personal information.

379. As a result of these revelations, Marriott's stock dropped by $6.81 from a close of $121.84 per share on November 29, 2018 to $115.03 per share on November 30, 2018, a decline of 5.59%.

380. Several outlets issued reports discussing the announcement of the Breach and resulting stock price decline. MarketWatch also reported that Marriott's stock price dropped "5.6% in premarket trade Friday, after the hotel operator disclosed a 'data security incident' of

its Starwood guest reservation database that contains information on up to 500 million guests." Additionally, Bloomberg reported that Marriott's stock "tumble[d]" on the revelation of the Breach, and Nasdaq.com reported that Marriott's "stock was falling hard" on news of the Breach.

X. APPLICATION OF PRESUMPTION OF RELIANCE

381. Lead Plaintiff is entitled to a presumption of reliance on Defendants' material misrepresentations and omissions pursuant to the fraud-on-the-market theory:

(a) Marriott's securities were actively traded on the NASDAQ and Chicago Stock Exchange, informationally efficient markets, throughout the Class Period;

(b) Marriott's securities traded at high weekly volumes during the Class Period;

(c) as a regulated issuer, Marriott filed periodic public reports with the SEC;

(d) Marriott regularly communicated with public investors by means of established market communication mechanisms, including through regular dissemination of press releases on the major news wire services and through other wide-ranging public disclosures, such as communications with the financial press, securities analysts and other similar reporting services;

(e) the market reacted promptly to public information disseminated by Marriott;

(f) Marriott's securities were covered by numerous securities analysts employed by major brokerage firms who wrote reports that were distributed to the sales force and certain customers of their respective firms. Each of these reports was publicly available and entered the public marketplace. The firms who wrote analyst reports on Marriott during the

Class Period include, but are not limited to, the following: Barclays, Deutsche Bank, JP Morgan, Jefferies, SunTrust Robinson Humphrey, Wells Fargo, and others;

(g) the material misrepresentations and omissions alleged herein would tend to induce a reasonable investor to misjudge the value of Marriott's securities; and

(h) without knowledge of the misrepresented or omitted material facts alleged herein, Lead Plaintiff and other members of the Class purchased shares of Marriott's securities between the time Defendants misrepresented or failed to disclose material facts and the time the true facts were revealed.

382. In the alternative, Lead Plaintiff is entitled to a presumption of reliance under *Affiliated Ute Citizens of Utah* v. *United States*, 406 U.S. 128 (1972), because the claims asserted herein against Defendants are predicated upon omissions of material fact which there was a duty to disclose.

XI. NO SAFE HARBOR

383. The statutory safe harbor provided by the PSLRA for forward-looking statements under certain circumstances does not apply to any of the materially false and misleading statements and omissions alleged herein.

384. ***First***, Defendants' statements and omissions alleged to be false and misleading relate to historical facts or existing conditions, and omissions are not protected by the statutory safe harbor. Defendants' false and misleading statements and omissions alleged herein are not forward-looking because such statements: (1) relate to historical or current fact; (2) implicate existing conditions; (3) do not contain projections of future performance or future objective; (4) the extent that any of the alleged false and misleading statements and omissions might be construed to touch on future intent, they are mixed statements of present facts and future intent and are not entitled to safe harbor protection with respect to the part of the statement that refers

to the present. To the extent that any of the alleged false and misleading statements and omissions might be construed to touch on future intent, they are mixed statements of present facts and future intent and are not entitled to safe harbor protection with respect to the part of the statement that refers to the present.

385. ***Second***, any purported forward-looking statements were not accompanied by meaningful cautionary language because any risks that Defendants warned of had already come to pass, and any cautionary language did not mention important factors of similar significance to those actually realized. Additionally, to the extent Defendants included any cautionary language, such language was not meaningful because any potential risks identified by Defendants had already manifested. To the extent Defendants included any cautionary language, it was not precise and did not relate directly to any forward-looking statements at issue. Defendants' cautionary language was boilerplate and did not meaningfully change during the Class Period, despite the fact that conditions had materially changed.

386. ***Third***, to the extent that there were any forward-looking statements that were identified as such, Defendants are liable because, at the time each of those forward-looking statements were made, the speaker knew the statement was false when made.

XII. CLASS ACTION ALLEGATIONS

387. Lead Plaintiff brings this federal securities class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of itself and all persons and entities that, during the proposed Class Period of November 16, 2015 through November 29, 2018, inclusive, purchased or otherwise acquired the publicly traded securities of Marriott, and were damaged thereby, except as excluded by definition. Excluded from the Class are: (1) Defendants; (2) members of the immediate family of each of the Individual Defendants; (3) any subsidiary or affiliate of Marriott, including its employee retirement and benefit plan(s) and their participants or

beneficiaries, to the extent they made purchases through such plan(s); (4) the directors and officers of Marriott during the Class Period, as well as the members of their immediate families; and (5) the legal representatives, heirs, successors, and assigns of any such excluded party.

388. The members of the Class are so numerous that joinder of all members is impracticable. According to Marriott's 2018 Annual Report, there were 340 million shares of Marriott's securities outstanding as of February 20, 2019 and over 36,4800 registered holders of such securities, with a significant number of shares held by banks, brokers and/or nominees for the accounts of their customers. While the exact number of Class members is unknown to Lead Plaintiff at this time and can only be ascertained through appropriate discovery, Lead Plaintiff believes that the proposed Class numbers in the thousands and is geographically widely dispersed. Record owners and other members of the Class may be identified from records maintained by Marriott or its transfer agent and may be notified of the pendency of this action by mail, using a form of notice similar to that customarily used in securities class actions.

389. Lead Plaintiff's claims are typical of the claims of the members of the Class. All members of the Class were similarly affected by Defendants' allegedly wrongful conduct in violation of the Exchange Act as complained of herein.

390. Lead Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class action and securities litigation.

391. There is a well-defined community of interest in the questions of law and fact involved in this case. Common questions of law and fact exist as to all members of the Class, and predominate over any questions solely affecting individual members of the Class. The questions of law and fact common to the Class include:

(a) whether the federal securities laws were violated by Defendants' acts and omissions as alleged herein;

(b) whether the statements made to the investing public during the Class Period contained material misrepresentations;

(c) whether Defendants' statements omitted material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading;

(d) whether Defendants knew or severely recklessly disregarded that their statements were false and misleading;

(e) whether and to what extent the market price of Marriott's securities was artificially inflated during the Class Period because of the material misstatements alleged herein;

(f) whether the Individual Defendants were controlling persons of Marriott;

(g) whether reliance may be presumed pursuant to the fraud-on-the-market doctrine and/or the presumption of reliance afforded by *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972); and

(h) whether the members of the Class have sustained damages as a result of the conduct complained of herein and, if so, the proper measure of damages.

392. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because, among other things, joinder of all members of the Class is impracticable. Furthermore, because the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

COUNT I

Violation of §10(b) of the Exchange Act and Rule 10b-5 Promulgated Thereunder Against All Defendants

393. Lead Plaintiff repeats, incorporates, and realleges each and every allegation set forth above as if fully set forth herein.

394. This Count is asserted pursuant to Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder by the SEC against all Defendants.

395. As alleged herein, throughout the Class Period, Defendants, individually and in concert, directly and indirectly, by the use of the means or instrumentalities of interstate commerce, the mails, and/or the facilities of national securities exchanges, made untrue statements of material fact and/or omitted to state material facts necessary to make their statements not misleading and carried out a plan, scheme and course of conduct, in violation of Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder. Defendants intended to and did, as alleged herein: (i) deceive the investing public, including Lead Plaintiff and members of the Class; (ii) artificially inflate and maintain the prices of Marriott's securities; and (iii) cause Lead Plaintiff and members of the Class to purchase Marriott's securities at artificially inflated prices.

396. The Individual Defendants were individually and collectively responsible for making the false and misleading statements and omissions alleged herein and having engaged in a plan, scheme and course of conduct designed to deceive Lead Plaintiff and members of the Class, by virtue of having made public statements and prepared, approved, signed and/or disseminated documents that contained untrue statements of material fact and/or omitted facts necessary to make the statements therein not misleading.

397. As set forth above, Defendants made their false and misleading statements and omissions and engaged in the fraudulent activity described herein knowingly and intentionally, or in such a severely reckless manner as to constitute willful deceit and fraud upon Lead Plaintiff and the other members of the Class who purchased Marriott's securities during the Class Period.

398. In ignorance of the false and misleading nature of Defendants' statements and omissions, and relying directly or indirectly on those statements or upon the integrity of the market price for Marriott's securities, Lead Plaintiff and other members of the Class purchased Marriott's securities at artificially inflated prices during the Class Period. But for the fraud, Lead Plaintiff and members of the Class would not have purchased Marriott's securities at such artificially inflated prices.

399. As set forth herein, when Defendants began to reveal adverse, previously undisclosed facts concerning the Company, the price of Marriott's securities declined precipitously and Lead Plaintiff and members of the Class were harmed and damaged as a direct and proximate result of their purchases of shares of Marriott's securities at artificially inflated prices and the subsequent decline in the price of shares of those securities when Defendants began to reveal such facts.

400. By virtue of the foregoing, Defendants are liable to Lead Plaintiff and members of the Class for violations of Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

COUNT II

Violation of §20(a) of the Exchange Act Against Certain of the Individual Defendants

401. Lead Plaintiff repeats, incorporates, and realleges each of the allegations set forth above as if fully set forth herein.

402. This Count is asserted pursuant to Section 20(a) of the Exchange Act against Defendants Sorenson, Oberg, Val Bauduin, and Linnartz.

403. As alleged above, Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder by making false and misleading statements in connection with the purchase and sale of Marriott's securities and by participating in a fraudulent scheme and course of business or conduct throughout the Class Period. This fraudulent conduct was undertaken with scienter and the Company is charged with the knowledge and scienter of each of Defendants Sorenson, Oberg, Val Bauduin, and Linnartz who knew of or acted with severely reckless disregard of the falsity of their statements and the fraudulent nature of this scheme during the Class Period. Thus, Marriott is primarily liable under Section 10(b) of the Exchange Act.

404. As set forth above, the Defendants Sorenson, Oberg, Val Bauduin, and Linnartz were controlling persons of Marriott during the Class Period, due to their senior executive positions with the Company and their direct involvement in the Company's day-to-day operations, as well as their ability to exercise and/or actual exercise of influence and control over the Company's dissemination of information.

405. By virtue of the foregoing, Defendants Sorenson, Oberg, Val Bauduin, and Linnartz each had the power to influence and control, and did influence and control, directly or indirectly, the decision-making of Marriott, including the content of its public statements with respect to the success of the due diligence and integration process of Starwood, and the effectiveness of it cybersecurity and compliance with industry and regulatory norms.

406. Defendants Sorenson, Oberg, Val Bauduin, and Linnartz acted knowingly and intentionally, or in such a severely reckless manner as to constitute willful fraud and deceit upon

Lead Plaintiff and the other members of the Class who purchased shares of Marriott's securities during the Class Period.

407. In ignorance of the false and misleading nature of the Company's statements and omissions, and relying directly or indirectly on those statements or upon the integrity of the market prices for shares of Marriott's securities, Lead Plaintiff and other members of the Class purchased shares of Marriott's securities at an artificially inflated price during the Class Period. But for the fraud, Lead Plaintiff and members of the Class would not have purchased shares of Marriott's securities at artificially inflated prices.

408. As set forth herein, when Defendants subsequently revealed adverse, previously undisclosed facts concerning the Company, the price of shares of Marriott's securities declined precipitously and Lead Plaintiff and members of the Class were harmed and damaged as a direct and proximate result of their purchases of shares of Marriott's securities at artificially inflated prices and the subsequent decline in the price of shares of those securities when such facts were revealed.

409. By reason of the foregoing, Defendants Sorenson, Oberg, Val Bauduin, and Linnartz are liable to Lead Plaintiff and the members of the Class as controlling persons of Marriott in violation of Section 20(a) of the Exchange Act.

XIII. PRAYER FOR RELIEF

410. WHEREFORE, Lead Plaintiff, on behalf of themselves and the Class, respectfully pray for judgment against Defendants as follows:

(a) Determining that this action is a proper class action maintained under Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure, certifying Lead Plaintiff as the Class Representative, and appointing Labaton Sucharow LLP as Class Counsel pursuant to Rule 23(g);

(b) Awarding Lead Plaintiff and the Class compensatory damages against all Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial together with prejudgment interest thereon;

(c) Awarding Lead Plaintiff and the Class their reasonable costs and expenses incurred in this action, including but not limited to attorneys' fees and costs incurred by consulting and testifying expert witnesses; and

(d) Granting such other and further relief as the Court deems just and proper.

XIV. DEMAND FOR TRIAL BY JURY

Lead Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: August 5, 2019

Respectfully submitted,

LABATON SUCHAROW LLP

By: */s/ Carol C. Villegas*

Carol C. Villegas
Mark S. Goldman*
140 Broadway
New York, NY 10005
Telephone: (212) 907-0700
Facsimile: (212) 818-0477
Email: cvillegas@labaton.com
Email: mgoldman@labaton.com
**Pro hac vice* application forthcoming

Attorneys for Lead Plaintiff and Lead Counsel for the Class

CERTIFICATE OF SERVICE

I, Carol C. Villegas, certify that, on August 5, 2019, I caused this document to be filed on all counsel of record by filing it electronically via the CM/ECF system.

/s/ *Carol C. Villegas*
Carol C. Villegas